Turbolinux®7 DataServer 用户指南

本手册由 Turbolinux Inc.设计和完成.

联系方式：

电 话: 86.10.65054020

传 真: 86.10.65054017

地址: 北京朝阳区光华路 7 号汉威大厦 15 层西区

邮政编码: 100004

网址: http://www.Turbolinux.com.cn/

前　言

致谢

Turbolinux7 DataServer 使用指南提供使用 Turbolinux7 DataServer 所需要的基本信息，该 Turbolinux 采用 Linux 2.4 内核，部分汉字字库采用汉仪字库.

感谢您从众多的 Linux 中选择 Turbolinux！

在日本、美国、中国 Turbolinux 公司的共同努力协作开发下 Turbolinux 具有安装简便、应用广泛、性能高、便于使用的特点.

自 1993 年以来，我们一直进行 linux 方面的工作，Turbolinux 在太平洋沿岸地区是 Linux 的带头羊.我们在 1997 年就推出了自己的国际化版本，目前支持简体中文，繁体中文、日文、朝鲜文以及美式英文.有关 Turbolinux 的最新信息，请访问我们的 Web 站点 *http://www.Turbolinux.com.cn/*.

通过开放源码运动以及 Linux 的缔造者 Linus Torvalds 的推动，我们的事业取得了成功；通过我们的共同努力,用户对 Turbolinux 感到满意.我们向那些已经而且继续为实现这一目标作出贡献的 Linus Torvalds 以及世界各地无数的 linux 开发者们表示感谢.

第一章　基本操作

本章将介绍 Turbolinux 的基本操作,如果您对这些很熟悉可以直接跳过.

1.1 系统登录

与其他形式的 UNIX 类似，如果要使用 Turbolinux，必须登录。Turbolinux 是多用户多任务的操作系统，每位合法用户都有也必须有唯一标识。登录过程是建立在用户身份识别基础上的。通过这种方式，允许合法用户访问系统，并将未授权的用户挡在系统之外。

Turbolinux 安装过程中，已经创建了超级用户(root)账户。在安装过程中或安装结束后，您都可以创建一些普通用户账户。

用户登录系统时，为了使系统能够识别自己，必须输入用户名和密码，经系统验证无误后方能进入系统

- 超级用户帐号 root :使用这个帐号能访问所有文件，可以在系统中做任何事情。大多数管理任务要求必须为 root 才应允。 在 Turbolinux 系统安装中会自动创建 root 帐号，请您牢记该账号的口令。
- 普通用户帐号： 这个帐号供普通用户使用，只能访问管理员所授予权限的文件，只能做管理员所授予的有限的操作。

用户登录进入系统后,如果是超级用户(root)提示行前面的符号是“ # ”,普通用户的提示符是“ $ ”。

超级用户帐号通常完成一些系统管理的工作。除非是测试系统，绝不要把超级用户帐号当普通帐号使用。 您应在需要时用 su 命令切换到 root 用户，完成后立即退回到普通用户。以免无意中破坏系统。

1.1.1　定义登录方法

安装 Turbolinux 安装过程中，默认登录方法是选择“ 基于文本的登录 ” 方法,该方法采用文本命令行方式进行系统登录,如果需要也可以选择 “基于图形的登录” 。文本登录是首先登录系统,然后用命令方式再启动 X Windows 图形界面。图形登录的登录界面将算在启动 X Windows 系统后图形界面中进行。

命令 xconfig(turboxcfg)，或 setup 工具中的 “配置 Xwindos 功能” 均可启动 X windows 图形配置工具，更改登录方法。

或者,您也可以直接修改配置文件 /etc/inittab 的改变登录方法。

1.1.2 使用命令行进行登录

用户登录分两步进行：第一步，输入用户的登录名，系统根据该登录名识别用户；第二步，输入用户的口令，该口令是用户自己选择的一个特定字符串，对其他用户保密，是系统辨别真假用户的关键。对于本例，主机名为 Turbo，用户名为 chris。

```
[Turbo] login: chris
Password: password
[chris@Turbo /home]$
```

出于安全方面的原因，系统不会显示密码字符串。

在上面的示例中，请注意主机名是如何从[hostname]变为[username@hostname /user_homedirectory]的，也就是说，从［Turbo］变为了［chris@Turbo /home］。

如果你是使用命令行来登录的，但却打算使用 X 图形界面，可以用下述命令来启动 X Windows 系统：

```
[chris@Turbo /home]$ startx
```

注意：超级用户应使用 **xconfig** 或 **turboxcfg** 命令已经配置好了你的 **XWindows** 系统, 普通用户没有这个权限.

1.1.3 在命令行下退出登录状态

退出登录状态，使用命令 logout 或 exit：

```
[chris@Turbo /home]$ logout
```

关闭计算机必须有超级用户的权限，然后运行 shutdown 或 halt 命令。

1.1.4 使用 GUI（图形化用户界面）进行登录

用图形登录过程由两个步骤组成，和基于文本的登录类似：

1． 在登录行上（Login：）输入用户名并按下回车键
2． 在密码提示符处键入密码，并按下回车键。当你成功登录系统后，X Window 开始启动，并显示 X Window 系统管理器桌面。

使用 GUI 退出登录：

如果打算从 X windows 环境退出，在主菜单下选择“Logout”，或用鼠标点击任务条上

的登录退出图标。

> **注意： 如你已从命令行进行登录，用 startx 启动，会直接进入 X window， 不再要求图形登录过程。**

1.1.5 虚拟终端

Turbolinux 设置有 6 个虚拟终端，您可以用 Alt-F1，Alt-F2，…Alt-F6 在它们之间做切换。

从 X Window 切换到虚拟终端，您应用 Ctrl-Alt-F? (F? 为 F1, F2, … F6 之一) 按键组合。一旦您从 X Window 切换到任一个虚拟终端之後， 您就可以只用 Alt-功能键来切换到其他虚拟终端。

Alt-F7 切回 X Window 。

1.1.6 关闭系统

只超级用户(root)才允许使用与关机有关的命令。对于使用 GNOME 窗口管理器的用户可以选择“退出登录”（Logout），然后出现关机选项菜单，其中包括“Halt”（停止）和“Reboot”（重新引导）等选项。简单地选择所需的选项，然后选择“确认”即可。对于使用 KDE 窗口管理的用户，需要在控制台使用命令“halt”或“shutdown”命令关闭系统。

1.2 账户管理

超级用户(root)账户具有特权，当以超级用户(root)身份登录到系统后，就能访问和运行任何程序，可以进行系统的配置和管理工作。 但超级用户(root)身份登录到系统也存在巨大的危险，可能会无意删除很重要的文件或破坏系统的正常工作。

要想安全地进行操作，应以普通用户身份登录到系统，只有需要时才使用 su 命令切换为超级用户身份，然后以超级用户(root)的特权执行完所需的任务，完成后立即退出超级用户(root)账户。

注意：对于超级用户(root)的账户和密码，应严格控制，防止非法入侵。

1.2.1 创建和更改用户账户（useradd, passwd）

安装 Turbolinux 的过程中会创建超级用户(root)账户。 普通用户账户可以在安装过程中

创建，也可以在安装完成后创建。

注意：只有超级用户才能创建用户以和更改其它用户的密码。一般的用户账户只能使用更改自己的密码。

创建新账户

要想创建账户 chris，密码为 jasper123。可使用下面给出的命令序列。在这个命令序列中，黑体表示的是用户的输入，非黑体表示的是系统的响应：

useradd chris
passwd chris
Changing password for user chris
New UNIX password: ***jasper123***
Retype new UNIX password: ***jasper123***
passwd: all authentication tokens updated successfully
#

注意：在上面的命令序列中，当你键入 jasper123 时，键入的字符串不会出现在屏幕上。这是一种基本的安全防范措施。

更改密码

如果 root 用户打算更改用户 chris 现在的密码，可以运行下面给出的命令序列。假定新密码是 bambi321：

passwd chris
Changing password for user chris
New UNIX password: ***bambi321***
Retype new UNIX password: ***bambi321***
passwd: all authentication tokens updated successfully

处理错误消息

当你设置密码时，可能会遇到下述错误消息中的一种，说明您设置的密码是不安全的密码，可能会造成安全漏洞：

BAD PASSWORD: it is too short	坏密码：太短	当你键入的密码字符串不到 6 个字符时，就会出现该消息，如“me”.
BAD PASSWORD: it is based on a dictionary word	坏密码 这是基于词典的单词	当你输入了词典中常见的单词时，就会出现该消息，例如“ system12”。
BAD PASSWORD: it is too simplistic/systematic	坏密码 过于简单/系统	当你输入的密码字符串太简单或太系统时，，就会出现该消息，例如“ abcdef123456”.

1.2.2 删除用户账户

要想删除用户账户，例如 chris，可以运行下述命令：

```
# userdel chris
```

使用-r 选项，还可以同时删除该用户的主目录，例如：

```
# userdel -r chris
```

注意：只有超级用户才能运行命令 userdel。

1.2.3 切换用户（su）

你可以直接从当前用户切换为另一名用户，而不必执行繁琐的退出登录然后再重新登录。例如，如果你从当前用户切换到用户 terri，可以执行下述命令序列：

```
$ su terri
Password: password
```

如果你想使用新的系统环境而不打算继续使用当前用户的用户环境,请添加一个“ - ”（减号）选项，后跟一个空格。

```
$ su - terri
Password: password
```

注意：超级用户(root)使用 su 命令，系统不会提示你输入用户密码。

使用命令 exit 或 Ctrl-d 返回到上一次使用的用户身份：

```
$ exit
```

exit

$

如果想切换到超级用户(root)身份，可使用命令 su，不必给出任何参数：

$ **su** -

Password: root_password

#

如果想了解当前用户的情况，运行下述命令：

$ **whoami**

terri

在上面的示例中，登录的用户是 terri。

1.3 关闭系统

对于 Unix 或 Turbolinux 系统最好使用命令正常关闭系统,否则可能造成系统或文件的丢失。如果在控制台环境下（即不在 X Window 系统中），请切换为超级用户，然后执行下述命令：

shutdown [options][time][message]

下面给出了可用的选项：

-h 停止（暂停）

-r 重新引导

如果使用使用时间参数，可以在一段时间后关闭系统：

xx.yy	在 xx 小时 yy 分钟关闭系统
+x	经过 x 分钟后，关闭系统
Now	立刻关闭系统

消息“message”如果省略将发出默认的信息，最好向每位已经登录的用户发送一则消息通知系统的关闭,让用户有充分的时间关闭自己的作业。例如，“The system will shutdown at 6 PM; please finish your work before then”（本系统将在下午 6 点关闭，请在此之前结束您手头的工作）。

shutdown -r +1

Broadcast message from root (pts/0) Fri Dec 14 11:50:33 2001...

The system is going DOWN for reboot in 1 minute !!

Broadcast message from root (pts/0) Fri Dec 14 11:51:33 2001...

The system is going down for reboot NOW !!

如果您确认系统上没有其他人登录或者出现某些紧急情况您可以立即下电:

\# **shutdown -h now**

或

\# **halt**

如果你处在 GNOME **环境中，可选择“** Logout **”（退出登录），从“** System **”（系统）菜单下选择“** Halt **”（停止）。**

或者您也可以开启控制台输入上述系统关闭指令.

注意：只有超级用户才能运行 shutdown 命令。

使用命令 halt**，会终止所有正在运行的进程。一旦屏幕上显示了下述消息，就可以切断机器的电源。**

The System is halted

重新启动系统

使用下述选项来运行 shutdown **命令重新启动系统：**

\# **shutdown -r now**

或

\# **reboot**

计算机将显示一则消息，通知你所有的进程均已被终止。然后系统会自动重新启动。

1.4 文件

用户的数据和程序大多以文件的形式保存。用户使用 Linux 系统的过程中，需要经常对文件和目录进行操作。

1.4.1 基本概念

在大多数操作系统中都有文件的概念。文件是 Linux 用来存储信息的基本结构，它是被命名（称为文件名）的，并存储在某种介质（如磁盘、光盘和磁带等）上的一组信息的集合。Linux 文件均为无结构的字符流形式。文件名是文件的标识，它由字母、数字、下划线和圆点组成的字符串来构成。用户应该选择有意义的文件名。Linux 要求文件名的长度限制在 255 个字符以内。

为了便于管理和识别，用户可以把扩展名作为文件名的一部分。圆点用于区分文件名和扩展名。扩展名对于将文件分类是十分有用的。用户可能对某些大众已接纳的标准扩展名比较熟悉，例如，C 语言编写的源代码文件总是具有 C 的扩展名。用户可以根据自己的需要，随意加入自己的文件扩展名。

以下例子都是有效的 Linux 文件名。

preface

chapter1.txt

xu.c

Linux 系统中有三种基本的文件类型：普通文件、目录文件和设备文件。

- 普通文件

普通文件是用户最经常面对的文件。它又分为文本文件和二进制文件。

文本文件：这类文件以文本的 ASCII 码形式存储在计算机中。它是以"行"为基本结构的一种信息组织和存储方式。

二进制文件：这类文件以文本的二进制形式存储在计算机中，用户一般不能直接读懂它们，只有通过相应的软件才能将其显示出来。二进制文件一般是可执行程序、图形、图像、声音等等。

- 目录文件

设计目录文件的主要目的是用于管理和组织系统中的大量文件。它存储一组相关文件的位置、大小等与文件有关的信息。目录文件往往简称为目录。

- 设备文件

设备文件是 Linux 系统很重要的一个特色。Linux 系统把每一个 I/O 设备都看成一个文件，与普通文件一样处理，这样可以使文件与设备的操作尽可能统一。从用户的角度来看，对 I/O 设备的使用和一般文件的使用一样，不必了解 I/O 设备的细节。设备文件可以细分为块设备文件和字符设备文件。前者的存取是以一个个字符块为单位的，后者则是以单个字符为单位的。

在计算机系统中存有大量的文件，如何有效的组织与管理它们，并为用户提供一个使用方便的接口是文件系统的一大任务。Linux 系统以文件目录的方式来组织和管理系统中的所有文件。所谓文件目录就是将所有文件的说明信息采用树型结构组织起来--即我们常说的目录。也就是说，整个文件系统有一个"根"（root），然后在根上分"杈"（directory），任何一个分杈上都可以再分杈，杈上也可以长出"叶子"。"根"和"杈"在 Linux 中被称为是"目录"或"文

件夹"。而"叶子"则是一个个的文件。实践证明，此种结构的文件系统效率比较高。

如前所述，目录也是一种类型的文件。Linux 系统通过目录将系统中所有的文件分级、分层组织在一起，形成了 Linux 文件系统的树型层次结构。以根目录为起点，所有其他的目录都由根目录派生而来。一个典型的 Linux 系统的树型目录结构如图 3.1 所示。用户可以浏览整个系统，可以进入任何一个已授权进入的目录，访问那里的文件。

各个目录结点"之下"都会有一些文件和子目录。并且，系统在建立每一个目录时，都会自动为它设定两个目录文件，一个是"."，代表该目录自己，另一个是".."，代表该目录的父目录，对于根目录，"."和".."都代表其自己。

Linux 目录提供了管理文件的一个方便途径。每个目录里面都包含文件。用户可以为自己的文件创建自己的目录，也可以把一个目录下的文件移动或复制到另一目录下，而且能移动整个目录，并且和系统中的其他用户共享目录和文件。也就是说。我们能够方便地从一个目录切换到另一个目录，而且可以设置目录和文件的管理权限，以便允许或拒绝其他人对其进行访问。同时文件目录结构的相互关联性使分享数据变得十分容易，几个用户可以访问同一个文件。因此允许用户设置文件的共享程度。

需要说明的是，根目录是 Linux 系统中的特殊目录。Linux 是一个多用户系统，操作系统本身的驻留程序存放在以根目录开始的专用目录中，有时被指定为系统目录。

从逻辑上讲，用户在登录到 Linux 系统中之后，每时每刻都"处在"某个目录之中，此目录被称作工作目录或当前目录（Working Directory)。工作目录是可以随时改变的。用户初始登录到系统中时，其主目录（Home Directory）就成为其工作目录。工作目录用"."表示，其父目录用".."表示。

用户主目录是系统管理员增加用户时建立起来的（以后也可以改变），每个用户都有自己的主目录，不同用户的主目录一般互不相同。

用户刚登录到系统中时，其工作目录便是该用户主目录，通常与用户的登录名相同。

用户可以通过一个"~"字符来引用自己的主目录。

例如命令

/home/WANG$ cat ~/class/software_1

和下面的命令

/home/WANG$ cat /home/WANG/class/software_1 意义相同。shell 将用用户主目录名替换"~"字符。 目录层次建立好之后，用户就可以把有关的文件放到相应的目录中，从而实现对文件的组织。

对文件进行访问时，需要用到 "路径"（Path）的概念。

顾名思义，路径是指从树型目录中的某个目录层次到某个文件的一条道路。此路径的主要构成是目录名称，中间用"/"分开。任一文件在文件系统中的位置都是由相应的路径决定的。

用户在对文件进行访问时,要给出文件所在的路径。路径又分相对路径和绝对路径。绝对路径是指从"根"开始的路径，也称为完全路径；相对路径是从用户工作目录开始的路径。

应该注意到，在树型目录结构中到某一确定文件的绝对路径和相对路径均只有一条。绝对路径是确定不变的，而相对路径则随着用户工作目录的变化而不断变化。这一点对于我们以后使用某些命令如 cp 和 tar 等大有好处。

用户要访问一个文件时，可以通过路径名来引用。并且可以根据要访问的文件与用户工作目录的相对位置来引用它，而不需要列出这个文件的完整的路径名。例如，用户 WANG 有一个名为 class 的目录，该目录中有两个文件：software_1 和 hardware_1。若用户 WANG 想显示出其 class 目录中的名为 software_1 的文件，可以使用下列命令：/home/WANG$ cat /home/WANG/class/software_1

用户也可以根据文件 software_1 与当前工作目录的相对位置来引用该文件。这时命令为：

/home/WANG$ cat class/software_1

1.4.2 列出文件和目录（ls）

使用命令 ls 可列出文件和目录，并了解到有关文件和目录的其他信息。它的格式如下：

$ ls [options] [file name] [directory name]

常用的选项有：

-l	不仅列出文件名，还应列出各文件的的全部细节信息。
-a	列出所有的文件，包括正常情况下隐含的文件。
-F	在文件名上附着一个符号，以显示文件的类型（可执行文件用星号“*”表示，目录用斜杠“/表示”），在 Turbolinux 中，ls 被设置为了 ls –F 的别名。

如果未指定文件或目录名，那么将列出当前目录下的文件和子目录。

在下面给出的示例中，介绍带有各种选项的 ls 命令,假设我们已经创建 jon 用户,并以该用户登录系统。对于这里给出的示例，ls 命令是在目录/home/jon 下运行的。

在 Turbolinux 中，下述命令等同于-F 选项：

```
$ ls /home/jon
nsmail/        foo1      foo2
```

在 Turbolinux 中，命令 ls 的作用与 ls–F 相同。仅显示文件和目录：

```
$ ls -l /home/jon
total 352
drwx------ 2 jon          jon 1024 Aug 27 01:01 nsmail/
-rw------- 1 jon          jon 356352 Aug 27 07:25 foo
```

显示每个文件和目录的详细信息：

```
$ ls -a /home/jon
./                 .bashrc            .lang/       .vimrc
../                .elvisrc           .less        .xemacs/
.ICEauthority      .exrc              .mc/         .xsession*
.Xdefaults         .gnome/            .rhosts      nsmail/
.bash_history      .gnome-desktop/    .sawfish/    foo
.bash_logout       .gnome_private/    .screenrc    foo1
.bash_profile      .inputrc           .tcshrc      foo2
```

显示当前目录下的所有文件和目录，包括隐含文件、目录、以及子目录。

1.4.3 切换工作目录（cd）

要想从当前目录切换到不同的目录，可使用 cd 命令。它的格式是：

cd [name of the desired directory]

如果你在使用 cd 命令时未带参数，即省略了目录名，那么命令 cd 将切换目录到当前用户的主目录下。

不必总是为所需的目录切换指定完整的路径。可以使用下述参数：

符号	意义
.	当前目录
..	当前目录的上一级目录即父目录
~	用户的主目录
-	当前目录的前一个目录

举例说明，如果打算将当前目录（/home/jon）切换为目录/home，可使用下面给出的两个命令之一：

$ **cd /home**

$ **cd ..**

注意 cd 和 .. 之间必须有空格

再举一例，如果打算将当前目录（/home）切换到用户的主目录，可使用下面给出的命令中的任何一种：

$ **cd /home/jon**

$ **cd ./jon**

$ **cd jon**

$ **cd** ~

$ **cd**

1.4.4 查看当前目录（pwd）

要想查看你当前所在的目录，可以使用 pwd 命令：

$ **pwd**

/home/jon

1.4.5 拷贝文件和目录（cp）

使用命令 cp，不仅能将文件从一个位置拷贝到另一个位置，而且还能将整个目录及其子

目录拷贝到不同的位置。命令 cp 的使用格式如下：

$ cp [options] [source filename | source directory name] [destination filename | destination directory name]

命令 cp 的常用选项如下：

-b　　如果目标文件已存在，在执行拷贝操作前，会对已存在的文件进行备份。

-f　　如果目标文件已存在，该文件将被强行覆盖。

-i　　如果目标文件已存在，系统会询问你是否要覆盖该文件。如果回答“ y ”（是），已存在的文件将被覆盖。如果给出的回答是“ y ”以外的，不会执行拷贝操作（在 TurbiLinux 中，cp 的别名被设为 cp-i）。

-u　　如果目标文件已存在，只有当目标文件的日期比源文件的日期更早时，才会执行拷贝操作（如果目标文件的日期较新，拷贝操作不会进行）。

-p　　在执行拷贝的过程中，保留源文件的属性（日期，所有者属性、许可权限）。

-v　　显示拷贝操作的结果（源文件名->目标文件名）。

-R　　拷贝目录

在下面的示例中，给出了 cp 命令与各种选项的使用方法，同时也包括系统响应：

$ **cp -v file1.txt file2.txt**

file1.txt -> file2.txt

使用-v 选项，会显示拷贝操作的结果。

$ cp -v file1.txt ../public

cp: overwrite ’../public/file1.txt’? y

file1.txt -> ../public/file1.txt

在这个例子中，由于 Turbolinux 命令 cp 的别名是 cp –i，而且存在具有相同文件名的目标文件，系统会询问你是否允许覆盖目标文件，如果你给出肯定的回答，拷贝将继续进行，并会显示拷贝的结果。

$ cp -rv directory1/ directory2/

directory1/ -> directory2/

整个目录“ directory1 ”被拷贝到了目录“ directory2 ”。

1.4.6　移动文件（mv）

使用命令 mv，可以将文件和目录从一个位置移动到另一个位置。它的使用格式是：

$ mv [options] [source filename | source directory name] [destination filename | destination

directory name]

下面给出了常用的选项：

-b　如果目标文件已存在，在执行移动操作前，会对已存在的文件进行备份。
-f　如果目标文件已存在，该文件将被强行覆盖。
-i　如果目标文件已存在，系统会询问你是否要覆盖该文件。如果回答“y”（是），已存在的文件将被覆盖。如果给出的回答是“y”以外的，不会执行移动操作（在 TurbiLinux 中，mv 的别名被设为 mv-i）。
-u　如果目标文件已存在，只有当目标文件的日期比源文件的日期更早时，才会执行移动操作（如果目标文件的日期较新，移动操作不会进行）。
-v　显示移动操作的结果（源文件名->目标文件名）。

例如，如果打算将文件 file1.txt 移动到目录../public 下，可以采用下述方式使用命令 mv：

$ **mv -v file1.txt ../public**

mv: overwrite ’../public/file1.txt’? **y**

file1.txt -> ../public/file1.txt

在这个例子中，存在具有相同文件名的目标文件，系统会询问你是否允许覆盖目标文件，如果你给出肯定的回答，移动将继续进行，并会显示移动的结果。

注意：如果你打算移动多个目录，但是却存在具有相同名称的目标目录，不会执行移动操作。

1.4.7 文件改名（mv）

使用命令 mv，你还能更改文件的名称，它的格式是：

$ mv [options] [source filename | source directory name] [destination filename | destination directory name]

常见的选项有：

-v　显示更改名称操作的结果（源文件名->目标文件名）。

例如，要想将文件名 file1.txt 更改为 file2.txt，可以按下述方式使用命令 mv：

$ **mv -v file1.txt file2.txt**

file1.txt -> file2.txt

如果你省略了-v 选项，将不会出现要求进行确认的系统响应。要想了解更多的信息，请参阅 mv 的 的 man page。

1.4.8 创建目录（mkdir）

使用命令 mkdir，可以创建新的目录。该命令的格式是：

$ mkdir [options] [name of the new directory]

该命令的常用选项有：

-m 在创建新目录的同时设置许可权限。

例如，如果打算在当前目录下创建目录“ mydirectory ”，可以按下述方式使用命令 mkdir：

$ **mkdir mydirectory**

$ **ls**

mydirectory/

在目录“ mydirectory/ ”中会出现斜杠“ / ”，这是因为在 Turbolinux 中，命令 ls 的别名被设置为了 ls-F。

1.4.9 删除文件和目录（rm, rmdir）

命令 rm 删除文件和目录。命令 rmdir 删除空目录。这两个命令的格式是：

$ rm [options] [name of file to delete | name of directory to delete]

$ rmdir directoryname

下面给出了常用的选项：

-f 强行删除,无提示。

-I 如果目标文件已存在，系统会询问你是否要覆盖该文件。如果回答“ y ”（是），已存在的文件将被覆盖。如果给出的回答是“ y ”以外的，不会执行移动操作（在 TurbiLinux 中，rm 的别名被设为 rm-i）。

-v 显示删除操作的结果。

-r 删除所有的文件、子目录和目录。

例如：

要想删除位于当前目录下的文件 file1.txt，可以按下述方式运行命令 rm：

$ rm -v file1.txt

rm: remove ’file1.txt’? y

在这个示例中，由于 Turbolinux 命令 rm 的别名被设为了 rm-i，而且你也对系统的询问作了肯定的回答“ y ”，因此该文件将被删除。

如果你打算删除目录“ /home/directory1 ”以及它的子目录，可以按下述方式使用 rm 命令：

$ rm -riv /home/directory1/

rm: descend into directory ’/home/directory1’? y

removing all entries of directory /home/directory1

rm: remove ’/home/directory1/file1.txt’? y

removing /home/directory1/file1.txt

rm: remove directory ’/home/directory1’? y

removing the directory itself: /home/directory1

如果打算删除空目录“directory2”**，可以按下述方式执行命令** rmdir**：**

$ rmdir directory2

在本例中，系统不会给出要求进行确认的提示。要想了解更多的信息，请参见 rmdir **的 的** man page**。**

1.4.10 查看文本文件（cat, less, more）

如果你打算查看文本文件的内容，可以使用命令 cat、less **和** more**。命令** cat **的格式是：**

$ cat [options] [name of file to view]

常用的选项是：

-n 　　**显示行号**

例如，如果希望显示文件/etc/lilo.conf **的内容，可以按下述方式使用命令** cat**：**

$ **cat -n /etc/lilo.conf**

1 boot=/dev/hda

2 map=/boot/map

3 install=boot/boot.b

4 prompt

5 lba32

6 imeout=50

7 default=linux

8 image=boot/vmlinuz

9 label=linux

10 root=/dev/hda6

11 initrd=/boot/initrd

12 read-only

使用命令 cat **时，一个长文件会在屏幕上滚动显示，你只能看到文件的末尾。这很不方便。如果你打算一个屏幕一个屏幕地显示长文件，命令** less **和** more **更为适合。命令** less **的格式是：**

$ less [options] [name of file to view]

使用 less 命令来查看文件时，可以使用数种击键命令，主要的击键命令如下：

击键命令	功能
空格	向下滚动一个屏幕
回车	向下滚动一行
Q	中断显示、退出
/<search pattern>	从当前屏幕开始，正向搜索“ search pattern ”。
N	重复搜索操作
D	向下滚动半屏
H	显示帮助信息
W	向上滚动一个屏幕
U	向上滚动半个屏幕
Y	向上滚动一行
? <string pattern>	从当前屏幕开始，逆向搜索“ search pattern ”。
N	从当前屏幕开始，重复执行前一次的逆向搜索操作
M	给出详细提示（与 more 类似），屏幕上最后一行的位置将以它在文件中的百分比表示。默认情况下，less 的提示是冒号“ : ”。
M	给出的提示比 m 更详细

例如，如果向显示文件/etc/X11/xinit/xinitrc 的内容，可按下述方式使用命令 less：

```
$ less /etc/X11/xinit/xinitrc
userresources=$HOME/.Xresources
usermodmap=$HOME/.Xmodmap
sysresources=/etc/X11/xinit/Xresources
sysmodmap=/etc/X11/xinit/Xmodmap
if [-f $sysresources ]; then
xrdb -merge $sysresources
fi
if [ -f $sysmodmap ]; then
xmodmap $sysmodmap
fi
if [ -f $userresources ]; then
/etc/X11/xinit/xinitrc 1/89 30%
```

如果在一个屏幕上仅显示了文件的部分内容，在屏幕的下方将出现一个状态行，在该行上将显示类似“ /etc/X11/xinit/xinitrc 1/89 30% ”的内容，它表示的是，已经显示的内容在文件中的百分比。当与-m 选项一起使用命令 less 时，就会显示百分比。

命令 more 是命令 less 的较早版本，其特性也不如 less 丰富，more 命令的格式是：

$ more [options] [name of file to view]

对于 more 命令，默认设置是给出 " 已显示内容的百分比 "。

1.4.11　查找文件（find）

要想查找、定位任何文件，可以使用 find 命令，该命令的格式是：

$ find [options] [path to search target] [expressions]

该命令的常用选项包括：

-name <string pattern>	搜索与<string pattern>匹配的文件
-iname <string pattern>	搜索与<string pattern>匹配的文件，忽略大小写之间的区别
-path <string pattern>	搜索与<string pattern>匹配的文件，包括完整的路径名
-ipath <string pattern>	搜索与<string pattern>匹配的文件，包括完整的路径名，忽略大小写之间的区别
-uid <user ID>	目标文件的数值用户 ID，用<user ID>指明
-user <user name>	目标文件的所有者，用<user name>指明
-gid <group ID>	目标文件的数值组 ID，用<group ID>指明
-group <group name>	目标文件所属的组，用<group name>指明

例如，如果打算搜索目录/etc 下结尾为.conf 的所有文件，可以键入下述命令：

```
$ find /etc -name "*.conf"
/etc/resolv.conf
/etc/ld.so.conf
/etc/X11/gdm/gdm.conf
.
.
/etc/smb.conf
/etc/yp.conf
/etc/lilo.conf
/etc/apcupsd.conf
/etc/esd.conf
/etc/xinetd.conf
```

设置<string pattern>时，可以使用通配符 " * " 和 " ? "。关于更多的信息，请参阅 find 的 的 man page。

1.4.12　搜索字符串（grep）

如果打算搜索文本文件中的文本字符串，应使用命令 grep，该命令的格式是：

```
$ grep [options] [string pattern for search] [target files]
```

该命令的常用选项包括：

-i	在搜索过程中，忽略大小写字符之间的区别
-l	不同于常规的搜索结果，仅列出文件的名称
-n	显示行的号码
-x	仅搜索与整个“string pattern”行相匹配的结果。

例如，如果打算在/etc/lilo.conf 下搜索包含字符串“boot”的所有文件，可以按下述方式使用命令 grep：

```
$ grep -n boot /etc/lilo.conf
1:boot=/dev/hda
2:map=/boot/map
3:install=/boot/boot.b
8:image=/boot/vmlinuz
11: initrd=/boot/initrd
```

其中，-n 选项可以在显示出的搜索结果上添加行号。

1.4.13 压缩和解压缩文件（gzip）

在很多场合下，你可能会希望通过压缩来降低大文件的尺寸。与该过程相反，有些时候，你可能需要对已经压缩的文件进行解压缩操作（已压缩的文件具有.gz 的扩展名）。执行这类任务时，可以使用命令 gzip。使用命令 gzip 的格式如下：

```
$ gzip [options] [file name]
```

该命令常用的选项有：

-d	解压缩文件。如果省略了-d 选项，将执行压缩操作。
-f	强制覆盖具有相同名称的文件
-v	以详细方式显示操作结果

例如，如果你打算压缩目录下所有的.txt 文件，并以详细方式显示结果，可以按下述方式使用 gzip 命令：

```
$ gzip -v *.txt
file1.txt: -82.6% -- replaced with file1.txt.gz
file2.txt: -53.0% -- replaced with file2.txt.gz
file3.txt: -72.2% -- replaced with file3.txt.gz
```

file4.txt: -75.3% -- replaced with file4.txt.gz
file5.txt: -66.5% -- replaced with file5.txt.gz

文件中的扩展名.gz **表示该文件已被压缩。**

现在，如果你打算对上一个示例中压缩的所有文件执行解压缩操作，可以按下述方式使用 gzip **命令：**

$ **gzip -dv *.gz**
file1.txt.gz: -82.6% -- replaced with file1.txt
file2.txt.gz: -53.0% -- replaced with file2.txt
file3.txt.gz: -72.2% -- replaced with file3.txt
file4.txt.gz: -75.3% -- replaced with file4.txt
file5.txt.gz: -66.5% -- replaced with file5.txt

1.4.14 创建和提取归档文件（tar）

使用命令 tar**，你可以将多个文件合并到一个单独的归档文件中。并且这些文件可以进行压缩处理。对于归档系统硬盘、移动硬盘或磁带上的重要数据来说，该命令十分有效。**

命令 tar **的使用格式是：**

$ tar [options] [file name of archive] [target file name]

命令 tar **能使用的常见选项包括：**

-c	**创建一个新的归档文件**
-f	**使用文件名来创建归档文件**
-v	**按详细方式列出已处理的文件**
-x	**从归档文件中提取文件**
-z	**使用** gzip**，在将文件添加到归档文件前对其进行压缩，或者是从归档文件中提取出文件后，对提取出的文件进行解压缩**

例如，如果你打算创建一个包含当前目录下所有.txt **文件的归档文件，可以按照下面给出的方式使用** tar **命令。**

$ tar -cvf file.tar *.txt
file1.txt
file2.txt
file3.txt
file4.txt
file5.txt

在上面所给的示例中，命令 tar **创建了一个名为** file.tar **的归档文件，在该归档文件中包含了所有列出的文本文件。**

现在，如果你打算从上一个示例中创建的归档文件中提取出所有的文件，可以按照下述方式使用 tar **命令：**

```
$ tar -xvf file.tar
file1.txt
file2.txt
file3.txt
file4.txt
file5.txt
```

在上面给出的示例中，命令 tar 将归档文件 file.tar 中的所有文件提取了出来，并同时显示在屏幕上。归档文件通常采用.tar.gz 形式的扩展名。对于这类文件来说，在对它们进行归档操作的同时可以使用 gzip 进行压缩处理。

如果您需要更高的压缩率可以考虑使用 bzip2 格式.

```
$ tar -czvf file.tar.gz  *.txt    ←---  包含 gzip 压缩的归档处理
$ tar -zxvf file.tar.gz           ←-----包含 gzip  解压缩的提取过程
file1.txt
file2.txt
file3.txt
file4.txt
file5.txt
```

1.5 进程管理

广义上的进程包括:由用户启动的进程、运行在后台的服务器服务、以及端口监控程序。由于 Turbolinux 是多用户、多进程的操作系统，因此进程管理很重要。在下面，我们介绍多种与进程管理有关的命令。

1.5.1 查出进程的状态（ps）

要想查出某一进程或多个进程的状态，可以使用 ps 命令。也可以使用命令 ps 来确定正在运行的进程。运行该命令的格式如下：

```
$ ps [options]
```

命令 ps 能使用的常见选项包括：

-a	显示由当前终端启动的所有进程
-f	以树形格式显示进程的层次结构
-l	显示详细列表（长格式）
-u	按用户定义的格式显示信息
-x	还应显示那些不是由当前终端（tty）启动的进程

例如，如果打算显示当前正在运行的所有进程，可以采用下述方式来运行 ps 命令：

```
$ ps -ax
PID     TTY     STAT     TIME     COMMAND
```

1	?	S	0:03	init
2	?	SW	0:00	[kflushd]
3	?	SW	0:00	[kupdate]
4	?	SW	0:00	[kpiod]
5	?	SW	0:00	[kswapd]
6	?	SW	< 0:00	[mdrecoveryd]
159	?	SW	0:00	[apmd]
169	?	S	0:00	syslogd -m 0
177	?	S	0:00	klogd
187	?	S	0:00	/usr/sbin/atd
197	?	S	0:00	crond
208	?	SW	0:00	[inetd]
214	?	S	0:00	/usr/sbin/sshd
252	?	SW	0:00	[dpkeyserv]
262	?	SW	0:00	[papd]
267	tty2	S	0:00	login -- root
268	tty3	SW	0:00	[mingetty]
269	tty4	SW	0:00	[mingetty]
270	tty5	SW	0:00	[mingetty]
271	tty6	SW	0:00	[mingetty]

要想以树形格式显示所有的当前进程，可按下述方式使用 ps **命令或使用命令** pstree**：**

$ **ps –axf**

$ pstree

如果打算了解更多的，请参阅 ps **的 的** man page**。**

1.5.2 终止进程（kill）

你可以有选择地终止当前正在运行的进程。要想执行该任务，可以使用 kill **或** killall **命令。命令** kill **的格式是：**

$ kill [options] [PID]

$ killall [OPTIONS] [--] name

其中 PID **表示进程** ID**，这是指定给进程的具有唯一性的号码。**

Killall **和** kill **的区别是** killall **使用进程名称**, kill **使用进程** ID **号码。**

如果在图形界面还可以使用 xkill **命令**,**然后用鼠标选择要终止的进程号码**.

常用的选项如下：

-l	**列出所有的信号名**
-<signal number>	**将由参数“ signal number ”（信号号码）指定的信号发送给进程。关于这些信号的详细信息，请参阅 kill 命令的 的 man page。**

例如，如果打算显示所有可用的信号号码以及它们的名称，可以按下述方式使用 kill **命**

令：

$ kill -l

1)	**SIGHUP**	**2)**	**SIGINT**	**3)**	**SIGQUIT**	**4)**	**SIGILL**
5)	**SIGTRAP**	**6)**	**SIGABRT**	**7)**	**SIGBUS**	**8)**	**SIGFPE**
9)	**SIGKILL**	**10)**	**SIGUSR1**	**11)**	**SIGSEGV**	**12)**	**SIGUSR2**
13)	**SIGPIPE**	**14)**	**SIGALRM**	**15)**	**SIGTERM**	**17)**	**SIGCHLD**
18)	**SIGCONT**	**19)**	**SIGSTOP**	**20)**	**SIGTSTP**	**21)**	**SIGTTIN**
22)	**SIGTTOU**	**23)**	**SIGURG**	**24)**	**SIGXCPU**	**25)**	**SIGXFSZ**
26)	**SIGVTALRM**	**27)**	**SIGPROF**	**28)**	**SIGWINCH**	**29)**	**SIGIO**
30)	**SIGPWR**	**31)**	**SIGSYS**	**32)**	**SIGTRMIN…**	**63)**	**SIGRTMAX**

如果省略了“ signal number **”（信号号码），**kill **命令会发送一条软终止信号（信号号码为** 15**，与** SIGTERM **对应）。**

例如，你可以按照下述方式，使用命令 kill **终止** PID **为** 555 **的进程，而无需指定信号号码（**signal number**）：**

$ kill 555

要想强行中止某一进程，可指定-9 **选项，它对应于信号“** SIGKILL **”：**

$ kill -9 555

注意：要想对某一进程执行 kill 命令，你必须具有超级用户的权限，或是该进程的所有者。

1.6 硬盘设备管理

与 UNIX 类似，Turbolinux 也将鼠标、硬盘驱动器、以及周边设备等均视作文件,是按反向树形结构来组织的。设备被当作文件对待,各种设备存在于互相连接的树形结构中,以根“ / ”作为起点和基础。对于硬盘、CDROM、软驱等设备（构成了互相连接的树形结构），通过“ mount ”（加载）命令进行设备加载/卸载。

1.6.1 硬盘分区

一个单独的物理硬盘必须被分割成一个或更多的分区，从逻辑上讲，这些分区是物理硬盘上的不同区域。

所谓分区，就是以逻辑方式对物理硬盘上的各个部分进行分配。通过这种方式，系统就能将一个物理硬盘视为多个磁盘。在微软的 DOS 和 Windows 操作系统下，为每个分区指定了单独的驱动器字母，例如驱动器 C、驱动器 D 等。Turbolinux 使用先进的文件树的概念，不存在这种字符驱动器，驱动器和分区均被当作文件对待，如下所示：

IDE 硬盘驱动器：

/dev/had primary drive（第 1 驱动器）

/dev/hdb primary slave（第 1 从属驱动器）

/dev/hdc secondary drive（第 2 驱动器）

/dev/hdd secondary slave（第 2 从属驱动器）

SCSI 硬盘驱动器：

/dev/sda

/dev/sdb

/dev/sdc

… 按 SCSI ID 排列

还包括分区信息：

/dev/hda1

/dev/hda2

/dev/hda3

…

1.6.2 分区和文件系统

不同的操作系统采用了不同的方式处理分区。DOS 和 Windows 系统采用 FAT 和 NTFS 文件系统，其中，每个分区的行为方式和表现是完全分理的。MacOS 操作系统，采用的文件系统是 HFS，OS/2 采用的是 HPPS。Turbolinux 采用了树形文件系统结构,不仅支持以上各种文件系统还支持 ext、ext2、ext3、reserfs 等几乎所有的文件系统种类,linux 是目前支持最多文件系统种类的操作系统。

这些文件系统各不相同，因此，不能在相同的分区上放置不同的文件系统。也就是说，要想让其他操作系统 Turbolinux 共存于相同的物理硬盘上，那么必须为每种操作系统划分独立分区。

例如，如果系统中已经存在包含 FAT 文件系统的分区，您不能在该分区上安装 Turbolinux。您必须为 Turbolinux 创建可以使用的分区。

只有对磁盘进行分区格式化之后才能在磁盘上安装系统或存储文件。Turbolinux DataServer 系统的安装过程中包括手动或自动磁盘分区过程,安装之前您可以不管磁盘是否已经完成分区。

如果您增加了一块磁盘,或者需要对原有的磁盘空间进行调整,您可能需要使用分区命令。

Turbolinux 系统中您可以使用 Linux 的 fdisk/cfdisk 程序创建或删除分区。

Turbolinux 推荐使用 fdisk。Linux 版本的 fdisk 程序采用了命令行界面。

注意：删除任何分区应格外小心，进行数据备份，分区删除后原先位于该分区上的所有数据均将丢失。

安装 Turbolinux 时，通常创建多个分区。最低程度，你需要创建一个根分区(root)和一个交换（swap）分区。交换分区被系统用作“虚拟内存”，用户不能访问该分区。

在很多情况下，除了根分区（root）和交换分区（swap）外，还可以创建多个其他分区。这些其他分区的设置，取决于你要运行的 Turbolinux 系统的类型。例如，如果有很多登录用户，最好在/home 下提供大量的可用空间。对于这种情况，最好创建一个/home 分区单独管理，以便更有效地利用硬盘空间;或者,为了使数据备份更加容易，你可能会考虑创建一个仅用于备份的分区，将数据备份从根目录分离出来。所有情况下均能良好工作的统一方案是不可能存在的。应当根据自己的实际需要，对硬盘进行具有自己特点的分区处理。在执行这类操作时，强烈建议预先制定一个分区计划。

1.6.3 使用 mount 命令

可以使用 mount 命令来访问各种文件和文件系统，包括 Turbolinux 系统上软盘驱动器和 CD-ROM,如果您正在 X 窗口系统使用 Turbolinux,您可以用鼠标点击桌面上的软驱或光驱图标直接访问软盘或光盘,加载过程将自动完成。下面给出了 mount 命令的格式。要想了解更进一步的细节，请参阅 mount 的 的 man page。

mount [options] [device to mount] [mount-point]

命令 mount **的常用选项有：**

-r	**加载文件系统，只读**
-w	**加载文件系统，读/写**
-v	**详细模式，显示当前的加载信息**
-t	**使用指定的文件系统类型进行加载**

一些常用的文件系统类型如下：

ext2	**在** Turbolinux **文件系统上使用标准** Linux **文件系统。**
ext3	**新的** Linux **文件系统。**
iso9660	CD-ROM **文件系统。**
Hfs	**标准** MacOS **文件系统。**
Hpfs	**标准** OS/2 **文件系统（只读）。**
Msdos	**标准** MS-DOS **文件系统（不支持长文件名）**
Vfat	**用于** MS-DOS **和** Windows 95/98 **的标准文件系统（支持长文件名）。**

Swap**用于交换分区的文件系统。**

使用下述命令加载软盘，可以读取 MS-DOS **格式的软盘：**

```
# mount -t msdos /dev/fd0 /mnt/floppy
```

可以使用如下命令直接访问 msdos **格式的软盘(不需上述的加载过程)：**

```
# mdir A:
# mcopy a:*.* .
# mdel a:*
```

在加载点/mnt/cdrom 处加载一个 CD-ROM**，可以使用下述命令：**

```
# mount -r -t iso9660 /dev/cdrom /mnt/cdrom
```

上面给出了该命令语法的通常格式。Turbolinux **的** CD-ROM（iso9660）**和软盘**（ext2）**的加载点在文件**/etc/fstab **中已经进行了设置，可以将** mount（**加载**）**命令简写为：**

```
# mount /mnt/cdrom
# mount /mnt/floppy
```

要想弹出 CD_ROM **或软盘，确认没有任何进程正在使用该设备后使用命令** unmount **卸载它：**

```
# umount /mnt/cdrom
# eject /mnt/cdrom
# umount /mnt/floppy
```

注意：

只有超级用户才能执行 mount（加载）和 unmount（卸载）命令

1.6.4 了解磁盘的使用情况（df, du）

命令 df 和 du 可以确定在硬盘上已使用了多少空间、剩余空间的多少。

使用命令 df，可以确定在一个或多个文件系统上（即分区上）有多少可用的磁盘空间。

使用命令 du，可以确定出单独的目录占用的磁盘空间，而不是文件系统所使用的磁盘空间。

使用 df 命令

使用 df 命令，可以确定在一个或多个当前加载的文件系统上有多少可用的磁盘空间。使用 df 命令的格式如下：

$ df [options] [target device name | target partition name | target directory name | target file name]

该命令会以块为单位（1024 字节）显示全部容量、已经使用的空间数量、可用的空间数量。同时显示的信息有:已使用的空间百分比、加载点。如果省略了目标，将显示与当前加载的所有分区有关的信息。

该命令常见的选项有：

-a	显示所有文件系统上的信息。
-k	以千字节为单位显示大小
-m	以兆字节为单位显示大小
-h	用 G（表示吉字节）、M（表示兆字节）后缀显示大小
-H	作用与-h 基本相同，差别在于采用的单位是“1000 字节”而不是“1024 字节”
-I	以信息节点为单位显示大小

在下面的示例中，给出了带不同选项的 df 命令的用法：

$ df

Filesystem	1k-blocks	Used	Available	Use%	Mounted on
/dev/hda2	1981000	193574	1685012	10%	/
/dev/hda6	1981000	14349	1864239	1%	/home
/dev/hda5	1981000	1099841	778747	59%	/usr

$ df -a

Filesystem	1k-blocks	Used	Available	Use%	Mounted on
proc	0	0	0	-	/proc
/dev/hda6	1981000	14349	1864239	1%	/home
/dev/hda5	1981000	1099841	778747	59%	/usr

$ df -k

Filesystem	1k-blocks	Used	Available	Use%	Mounted on
/dev/hda2	1981000	193574	1685012	10%	/
/dev/hda6	1981000	14349	1864239	1%	/home
/dev/hda5	1981000	1099841	778747	59%	/usr

$ df -m

Filesystem	1M-blocks	Used	Available	Use%	Mounted on
/dev/hda2	1935	189	1645	10%	/
/dev/hda6	1935	14	1820	1%	/home
/dev/hda5	1935	1074	760	59%	/usr

使用 du 命令

使用 du 命令，可以了解在每个目录已经占用的空间状况。使用 du 命令的格式如下：

$ du [options] [target directory name | target file name]

在指定的目录下，将以块为单位显示各文件的大小。如果省略了目标，将显示与当前目录有关的信息。

该命令常见的选项有：

-a	显示所有文件的计数，不仅仅是目录。
-b	以字节为单位显示大小
-c	在最后一行上显示目标的全部大小
-k	以千字节为单位显示大小
-h	用 G（表示吉字节）、M（表示兆字节）后缀显示大小
-H	作用与-h 基本相同，差别在于采用的单位是“1000 字节”而不是“1024 字节”

下面给出了单独使用命令 du，以及与选项-b（字节）一起使用 du 命令的示例：

```
$ du /home
    12        ./lost+found
    776       ./ftp/lib
    1         ./ftp/pub
    778       ./ftp
    22        ./httpd/cgi-bin/man
    142       ./httpd/cgi-bin
    136       ./httpd/icons
    17        ./httpd/aux/man
    18        ./httpd/aux
    1735      ./httpd
    1         ./gopher
    1         ./samba
    193       ./public
    1         ./nfs
    14002     .

$ du -b /home
    12288     ./lost+found
    794624    ./ftp/lib
    1024      ./ftp/pub
    796672    ./ftp
    22528     ./httpd/cgi-bin/man
    145408    ./httpd/cgi-bin
    48128     ./httpd/html/manual/images
    1472512   ./httpd/html
    37888     ./httpd/icon/small
    139264    ./httpd/icons
    17408     ./httpd/aux/man
    18432     ./httpd/aux
    1776640   ./httpd
    1024      ./gopher
    1024      ./samba
    197632    ./public
    1024      ./nfs
    14338048  .
```

1.7 安装和升级软件包

Turbolinux 采用 rpm 作为自己的软件包管理器，该管理器能提供一个有效的管理环境，在这个环境下，你可以安装、卸载、升级、或检查软件包。此外，它还能对软件包之间的关联性进行管理。

可以使用 Turbolinux 的软件包管理工具 turbopkg，也可以在命令行使用 rpm 命令管理软件包。

注意，对于很多软件包言，需要超级用户的权限才能安装。

Turbolinux 的软件包保存在目录光盘目录 turbo/RPMS/下。

使用 rpm 命令的格式如下：

$ rpm [options] [RPM package name]

命令 rpm 的常见选项有：

-I	安装
-U	升级
-e	删除
-h	用混编字符“#”标志显示进展状态
-v	详细显示（与-h 一起使用可获得更好的显示效果）
-q	查询当前已经安装的软件包

RPM 使用示例

了解已经安装的 rpm 软件包有关的信息：

```
# rpm -q apache
apache-1.3.20-6.i386.rpm
```

如果未安装该软件包，会出现下述消息：

package apache is not installed （未安装软件包 Apache）

查看已经安装的某个软件包的文件的列表：

```
# rpm -ql apache
/etc/httpd
/etc/httpd/conf
/etc/httpd/conf/access.conf
.
.
. <lines omitted>
/var/www/icons/uuencoded.gif
/var/www/icons/world1.gif
/var/www/icons/world2.gif
```

卸载软件包：

```
# rpm -e apache
```

安装软件包(假设当前当前目录包含该软件包)：

rpm -ivh apache-[version]

升级软件包(假设当前当前目录包含该软件包)：

rpm -Uvh apache-[new-version]

查看已经安装所有软件包列表：

rpm -qa

filesystem-2.0.10-1

bash-2.05-2

db1-1.85-25

gdbm-1.8.0-4

……..

………

xscreensaver-3.33-1

ZWinPro-3.3-9

zip-2.3-2

显示与 Apache **软件包有关的信息：**

rpm -qi apache

Name **（名称）**	: apache	Relocation : (not relocateable) **（重新布置：不能）**
Version **（主版本）**	: 1.3.20	Vendor : Turbolinux **（销售商）**
Release **（次版本）**	: 6	Build Date : Tue 04 Sep 2001 05:19:49 **（创建日期：）**
Install date **（安装日期）**	: Tue 02 Oct 2001 06:42:12 AM PDT	Build Host : cathedral.jp.tlan **（建立的主机：）**
Group **（组）**	: System Environment/Daemons **（系统环境／端口监控程序）**	Source RPM : apache-1.3.20-6.serc.rpm **（源** RPM **：）**
Size **（大小）**	: 1127235	License : Freely distributable and usable **（许可：自由发布和使用）**
Packager **（包装商）**	Turbolinux	
URL	: http://www.apache.org/httpd.html	
Summary **（概述）**	: The most widely used Web server on the Internet **（**Internet **上使用最广泛的** Web **服务器）**	
Description **（描述）**	: Apache is a powerful, full-featured, efficient and freely-available Web server. Apache is also the most popular Web server on the Internet **（**Apache **是一种强大的、具有完整特性的、高效的、和免费的** Web **服务器。**Apache **还是** Internet **上最流行的** Web **服务器）**	

注意：

在安装 CD 上，rpm 软件包位于目录 turbo/RPMS/下。首先，必须将 CD-ROM 加载为 /mnt/cdrom。多数软件包只有超级用户才能安装。

1.8 访问在线手册(man page)

Turbolinux 系统提供了大量命令和许多实用工具软件，这里由于篇幅的关系，主要介绍了 Turbolinux 的一些常用命令和实用软件。读者可以使用系统提供的联机帮助手册获取更多的信息。

Turbolinux 系统的联机手册(man page)中有大量的可用信息，根据其内容分成若干节。在 Linux 联机帮助手册上，几乎每个命令都有说明。因此，当用户对于 Linux 上的一个命令不会用或是不太了解时，就请使用联机帮助命令。

1.8.1 man 命令

这个命令应该是每个 Linux 系统上都有的。它格式化并显示在线的手册页。通常使用者只要在命令 man 后，输入想要获取的命令的名称(例如 ls)，man 就会列出一份完整的说明，其内容包括命令语法、各选项的意义以及相关命令等。

该命令的一般形式为：

man [选项] 命令名称

命令中各选项的含义分别为：

-M 路径 指定搜索 man 手册页的路径，通常这个路径由环境变量 MANPATH预设，如果在命令行上指定另外的路径，则覆盖 MANPATH的设定。

-P 命令 指定所使用的分页程序，缺省使用/usr/bin/less–is，在环境变量 MANPAGER 中预设。

-S 章节 由于一个命令名称可能会有很多类别，至于类别，列出如下：

1 一般系统的命令

2 系统调用的命令

3 C 语言函数库的命令

4 有关驱动程序和系统设备的解释

5 配置文件的解释

6 游戏程序的命令

7 其他的软件或是程序的命令

8 有关系统维护的命令

9 内核例程

-a 显示所有的手册页，而不是只显示第一个。

-d 这个选项主要在检查时使用，如果用户加入了一个新的文件，就可以用这个选项检查是否出错，这个选项并不会列出文件内容。

-f 只显示出命令的功能而不显示其中详细的说明文件。

-w 不显示手册页，只显示将被格式化和显示的文件所在位置。

例如：查看 cd 命令的使用方法。

$ man cd

如果需要查看 shell 命令 open 的帮助可以使用命令:

man 1 open
man open

如果需要查看编程函数 open 的帮助可以使用命令:
man 2 open

可以按 q 键退出 man 命令。使用命令 man 浏览信息的方式与使用 less 命令的极其相似。

1.8.2 help 命令

help 命令用于查看 Shell 命令的用途。用户可以通过该命令寻求 Shell 命令的用法，只需在所查找的命令后输入 help 命令，就可以看到所查命令的内容了。

例如：查看 od 命令的使用方法。

$ od --help

1.8.3 whereis 命令

这个程序的主要功能是寻找某命令所在的位置。例如，我们最常用的 ls 命令，它是在/bin 这个目录下的。如果希望知道某个命令存在哪一个目录下，可以用 whereis 命令来查询。

该命令的一般形式为：

whereis [选项] 命令名

说明：一般直接使用不加选项的 whereis 命令，但用户也可根据特殊需要选用它的一些选项。

该命令中各选项的含义分别为：

b 只查找二进制文件

m 查找主要文件

s 查找来源

u 查找不常用的记录文件

例如：查找 ls 命令在什么目录下。

$ whereis ls

ls:/bin/ls/usr/man/man1/ls.1

第二章　TCP/IP 网络

本章将描述 TCP/IP 网络的基本概念结构以及术语。

安装 Turbolinux 的过程中，已经执行了多种配置任务，如设置网络接口等。运行不同的服务器程序，必须完成不同的配置任务。通过本章，将在更高层次上理解 TCP/IP 网络以及它的某些基本组件。

2.1　TCP/IP

TCP/IP 是传输控制协议/Internet 协议的首字母缩写。结合这两个协议就能够在网络上（包括 Internet 上）的两台或多台计算机之间提供数据传输服务。下面，给出了对这两个协议工作方式的简要描述。

・在源计算机处，TCP 协议将数据信息分割成多个数据报，添加题头，并为每个分割后的单元添加序列号。然后将这些单元封装成数据包递送给 IP 协议。

・IP 协议负责创建信息包，每个信息报中均包含源 IP 地址和目标 IP 地址、物理地址、以及 TCP 数据报。然后，IP 协议将这些信息包递送给数据链路层，数据链路层负责将这些信息包递送到目标地址。

・在目标计算机处，IP 协议负责检查是否已收到完整无缺的信息包，并将收到的信息报向上递送给 TCP 协议。不过，IP 协议并不检查数据片段本身的完整性。

・TCP 协议会对信息包进行数据完整性检查、按照正确的顺序将这些信息包组装起来，将其准确恢复成原始的状态，然后将它们送到目标计算机上。

TCP 协议与开放式系统互联（OSI）模型的传输层对应，IP 协议对应于 OSI 模型的网络层。IP 协议不保证信息包内数据的完整性。这项任务由 TCP 协议负责。

2.2　以太网

以太网最早是在上个世纪 70 年代末由施乐（Xerox）公司开发的。目前（在本手册中讨论）的以太网版本是版本 2，它是由施乐（Xerox）、DEC 和 Intel 共同制定的标准，对应于 IEEE802.3 标准。

以太网采用了总线或星型拓扑，并采用了 CSMA/CD 来管理网络通信量。在一个以太网网络上，各个节点（计算机、打印机等）通过同轴电缆、光缆或双绞线链接在一起。

TCP/IP 协议组是众多 Internet 协议组中的一种。不过对于以太网网络而言，TCP/IP 协议组已经成为了事实上的数据通信标准。它将要从一个节点发送到另一个节点的所有数据分割

成多个信息包，在每个信息包中插入题头和报尾，并将这些信息包递送给硬件设备，由硬件设备完成传输。在信息包的题头中包含源地址和目标地址，以及其他信息。

在以太网网络上，每个节点会不断检查在网络上传递的每个信息包，而且仅接收那些明确发送给自己（本节点）的信息包或发送给多个节点的广播信息包。当采用了交换式网络集线器或路由器时，交换式网络集线器或路由器能够检查信息包的目标地址，并将信息包传送给另一个网络或子网。

2.3 CSMA/CD 协议

CSMA/CD（带有冲突检测的载波侦听多路存取）协议是用于以太网传输的多种协议中的一种。很多情形下，多台主机会试图同时传输数据，该协议能够处理这类情形。如检测到信息包“碰撞”，延迟一个随机时间后会再次发送,直到没有发现碰撞为止。CSMA/CD 协议会不断地监测物理网络电缆（载体），如果发现在网络上存在“交通堵塞”，就不会传输信息包。它将等待，直到网络上的“交通堵塞”解除为止，随后才会传输信息包。这种传输机制“碰撞”在所难免,同一网络上主机越多、网络信息越繁忙碰撞也就越多。

通过 CSDA/CD 协议，构建一个支持大量计算机和其他设备的网络,在极端的情况下，碰撞的数量会导致网络性能的急剧降低。但是，通过使用路由器或交换式网络集线器，将一个较大的网络分割成数个较小的网络，就能够避免这种情况。

2.4 MAC 地址

在以太网网络上，IP 地址是一种逻辑地址，而介质访问控制地址（或 MAC 地址）则是指定给每个网络接口卡（NIC）的唯一的实质地址(全球唯一的物理地址)。每个节点都会创建并维护一个特定的地址表，在这个地址表中包含了 IP 地址以及对应的 MAC 地址。单独的节点会使用地址解析协议（ARP）创建这个地址表。

MAC 地址是一个 6 字节的数字，遵循 IEEE 规则。前三个字节是制造商的号码，后三个字节是制造商为该单元提供的唯一的标识号码。没有两块正常生产 NIC（网络接口卡）会具有相同的 MAC 地址。

在 Linux 系统下，运行命令 ifconfig（HWaddr 就是 MAC 地址），可以确定 NIC 卡的 MAC 地址。

```
# ifconfig eth0
eth0    Link encap:Ethernet HWaddr 00:20:AF:??:??:??
inet addr:192.168.1.2 Bcast:192.168.1.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:0 errors:) dropped:0 overruns:0 frame:0
TX packets:14 errors:0 dropped:0 overruns:0 carrier:0
collisions:0
```

注意：双问号标志“？？”指任何数字值。

2.5 ARP

ARP（地址解析协议）主要用于查询对应 IP 地址的 MAC 地址。在系统启动时，每台主机仅知道对应自己 IP 地址的自己 MAC 地址。要想与另一台主机进行通信，该主机必须知道另一台主机的 MAC 地址。这时，该主机会发布一条 ARP 请求，另一台主机会用其自己的 MAC 地址予以应答,这个应答的 MAC 地址将被保存在发出查询的主机的高速缓冲区中。通过使用命令 arp，就能得知高速缓冲区中的这些内容

```
# arp -a
cdmaker.dev.cn.tlan (172.96.68.7) at 00:00:E8:77:CB:AC [ether] on eth0
ns.dev.cn.tlan (172.96.68.1) at 00:10:5A:82:C2:2C [ether] on eth0
```

2.6 IP 地址

IP 地址是一种逻辑地址，用于将 Internet 上的一台机器与其他机器进行区分。目前，IP 地址采用的是 IPv4 体系。在这个体系中，每个 IP 地址的长度为四字节。字节之间句点与下一个字节分隔,每字节的取值范围是 0-255,例如：192.168.1.2。

IP 地址由两部分组成：网络地址部分和主机地址部分。对位于相同网络上的每台主机来说，它们 IP 地址的网络地址部分是相同的。

要想更进一步地理解 IP 定址体系，就有必要理解网络掩码、网络地址、广播地址、以及网络分类。

网络掩码是一个长度为四字节的数字值，由带点符号的十进制数或十六进制数指明。例如：255.255.255.0(十进制)或 0xFF.0xFF.0xFF.0x00(十六进制)。如果将网络掩码的值转换为由多个二进制“0”和“1”组成的序列，就更容易理解网络掩码的工作机制。IP 体系使用网络掩码，在 IP 地址上执行逻辑“与”(AND）计算操作。计算结果是对应于网络掩码中“1”的所有二进制位保持不变，而对应于网络掩码中“0”的所有二进制位将变为“0”。

例如，如果使用的 IP 地址是 192.168.1.2，网络掩码是 255.255.255.0；那么它的网络部分是 192.168.1，主机部分是 2。在有些情况下，网络掩码的比特数（位数）会附在 IP 地址上，从而得到 192.168.1.2/24。

简单的也可以这样理解:IP 地址对应掩码 255(二进制全 1)部分的字节就是网络地址.

网络是很复杂的,不可能用很短的篇幅讲解明白,如果您对网络很有兴趣,建议去读网络的专业书籍.

另一个重要的概念是广播地址。IP 地址的主机部分均是二进制的“1”时(不包括网络部分)，它就成了广播地址。广播地址用于网络信息的广播（将相同的信息包发送给同一网络上的所有主机）。例如，在网络 192.168.1 上，广播地址是 192.168.1.255。不仅如此，所有二进制位均为“1”的地址（255.255.255.255）也是广播地址。

如果 IP 地址是 255.255.255.255，它仅适用于同一网络内部的广播，但是，如果指定一个特殊的网络地址，网络地址就能够被用于广播。

ARP（地址解析协议）以及 DHCP（动态主机配置协议）等协议都需要使用广播地址解析主机的 IP 地址。应用程序或人为发送广播数据信息也是可能的。不过，这种“练习”会很快地堵塞网络，并使网络性能明显降低。

注意,广播地址不能被用作主机的 IP 地址。

命令 ifconfig 查看网络信息时包括网络掩码和广播地址。在该命令的输出结果中，“inet addr”是 IP 地址，“Bcast”是广播地址，“Mask”是网络掩码。

```
# ifconfig eth0
eth0 Link encap:Ethernet HWaddr 00:20:AF:??:??:??
inet addr:192.168.1.255 Bcast:192.168.1.255 Mask:255.255.255.0
```

开始时，IP 地址的网络部分由 8 个二进制位组成，主机部分是 24 个二进制位。这是基于这样一种观点：即人们能够管理数量不多的大型网络。但是，随着对中型网络和小型网络需求的日渐增加，这种 IP 地址类型难以胜任。为了解决这种问题，人们为 IP 地址引入了分类概念：A 类（大型网络）、B 类（中规模网络）、和 C 类（小规模网络）。

如下所示：

类	二进制最高两位	地址范围	网络掩码
A	00	0.0 – 127.255.255.255	255.0.0.0
B	10	128.0.0.0 – 191.255.255.255	255.255.0.0
C	11	192.0.0.0 – 223.255.255.255	255.255.255.0

A 类网络能容纳多达 16,770,000 台主机，B 类网络约能容纳 65000 台主机，而 C 类网络能容纳 256 台主机（实际上最多 254 台）。目前，个人和小型公司的低成本、永久性网络连接日渐普及，这样小于 C 类的网络（可被视为子网）随之日渐流行。这种类型的网络的网络掩码不随每个字节而变，而是随着二进制位而变化，因此对网络掩码和网络的计算变得更加复杂。在下面的示例中，介绍了针对某一子网的网络掩码设置。

名称	地址	最低位字节（以比特为单位）
主机	200.200.200.100/28	01100100
网络掩码	255.255.255.240	11110000
网络地址	200.200.200.96	01100000
广播	200.200.200.11	01101111

Internet 上，IP 地址由 InterNIC 组织管理分配。但在建立一个不直接连接到 Internet 的网络时，你可以从保留给本地局域网络使用的专有地址中选择 IP 地址。从这些内部网访问 Internet，必须有代理（Proxy）或使用地址伪装(IP Masquerade)。从 Internet 无法访问这些内部网 IP 的主机。

在 RFC（Internet 标准草案）中指定的局域网地址范围是：

类型	地址范围	网络掩码
A	10.0.0.0 – 10.255.255.255	255.0.0.0
B	172.16.0.0 – 172.31.255.255	255.255.0.0
C	192.168.0.0 – 192.168.255.255	255.255.255.0

2.7 网关地址

在以太网环境中，位于同一个网段中的主机能直接进行通信。如不同网段或不同网络中的主机进行通信，必须经由路由器。路由器具有两个或多个接口同不同的网络相连。每一接口，均分配有 IP 地址。该 IP 地址称为网关地址， 当目的主机不在同一网段内时，IP 包被送到网关，由路由器来转送。不同网络的网关地址不同。

2.8 网络启动过程

在前面的部分中我们已经介绍了多种概念，在下面的部分中，我们将具体解释与其他主机所进行的通信进程，该进程是在系统引导时被设置的。

Turbolinux 7 DataServer 采用脚本/etc/rc.d/init.d/network 设置自己的网络接口（实际上，它调用位于/etc/sysconfig/network-scripts 下的配置脚本)。通过这个脚本，你可以根据各种网络配置文件设置灵活的网络接口，根据系统 V 运行 init 进程。基本说来，一旦正确执行该脚本，就可以与其他主机进行通信。

执行/etc/rc.d/init.d/network 脚本设置网络接口时，将自动执行下面描述的步骤。

设置网络接口

1． 使用 ifconfig 命令，设置以太网设备的 IP 地址。

```
# ifconfig eth0 192.168.0.10 broadcast 192.168.0.255 netmask 255.255.255.0
```

2． 使用命令 route，设置网络地址。

```
# route add -net 192.168.0.0
```

3． 使用命令 route，设置默认网关

```
# route add default gw 192.168.0.1
```

要想使用 ifconfig 命令对网络配置进行任何永久性更改，需要编辑文件/etc/sysconfig/network-scripts/ifcfg-eth?等文件，并为 lo、IP 地址、广播地址和网络掩码设置正确的值。保存所编辑的文件。当下次引导系统时，这些新的 ifconfig 设置就会生效。

在 turbolinux 您还可以使用网络配置工具进行配置。

事实上，在第 1 个步骤前已经识别出网卡设备（这里是 eth0,通常可以自动识别）。你可以运行命令 dmesg 来检查已经识别出的网卡。Turbolinux 已经将常用的网卡驱动程序构建到了内核中，在启动时，会自动识别出相应的网卡设备。

注意：在上面的解释中，假设了这样一种环境，在此环境中具有一台正确配置了 IP 地址、DNS 服务器地址等的机器，在机器上运行着一块毫无问题的 NIC，而且该 NIC 卡和网络设备正确地连接在了一起。

2.8.1 检查网络

在某些时侯，出于某种原因网络可能会不工作。出现这种情况时，你可以采用下面介绍的步骤，检查网络的运行情况。

1． **检查是否已正确地识别出了 NIC 驱动程序并读取了该驱动程序：**

```
# lspci
00:00.0 Host bridge: Intel Corporation 440BX/ZX - 82443BX/ZX Host bridge (rev 03)
00:01.0 PCI bridge: Intel Corporation 440BX/ZX - 82443BX/ZX AGP bridge (rev 03)
00:07.0 ISA bridge: Intel Corporation 82371AB PIIX4 ISA (rev 02)
00:07.1 IDE interface: Intel Corporation 82371AB PIIX4 IDE (rev 01)
00:07.2 USB Controller: Intel Corporation 82371AB PIIX4 USB (rev 01)
00:07.3 Bridge: Intel Corporation 82371AB PIIX4 ACPI (rev 02)
00:10.0 Ethernet controller: 3Com Corporation 3c905B 100BaseTX [Cyclone] (rev 64)
00:14.0 SCSI storage controller: Adaptec AHA-2940U2/W / 7890
01:00.0 VGA compatible controller: nVidia Corporation Vanta [NV6] (rev 11)
# lsmod
Module          Size        Used by
nfs                          71712     1    (autoclean)
nfsd                         65792     8    (autoclean)
lockd                        47312     1    (autoclean)  [nfs  nfsd]
sunrpc                       63968     1    (autoclean) [nfs nfsd lockd]
3c59x                        25504     1    (autoclean)
aic7xxx                     105712     6
sd_mod                        9920    12
```

lspci **命令可以列出系统的硬件设备,找到我们需要的网卡信息。** lmod **命令可以检查该设备的模块是否已经正确加载。**

上面的系统响应表明，已经读取了针对 3Com 3c90x NIC **的** 3c59x **模块。**

如果在这个阶段，没能读取驱动模块，可使用命令 modprobe **读取针对** NIC **的驱动模块。**

```
# modprobe 3c59x
```

2． **使用命令** ifconfig**，检查是否已经正确地配置了网络接口。命令** ifconfig -a **会显示系统上所有的接口：**

```
# ifconfig -a
eth0 Link encap:Ethernet HWaddr 00:60:08:??:??:??
inet addr:192.168.1.2 Bcast:192.168.1.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:10559536 errors:0 dropped:0 overruns:0 frame:0
TX packets:1135365 errors:0 dropped:0 overruns:0 carrier:0
```

```
collisions:0
lo Link encap:Local Loopback
inet addr:127.0.0.1 Bcast:127.255.255.255 Mask:255.0.0.0
UP BROADCAST LOOPBACK RUNNING MTU:3584 Metric:1
RX packets:101202 errors:0 dropped:0 overruns:0 frame:0
TX packets:101202 errors:0 dropped:0 overruns:0 carrier:0
collisions:0
```

要想与其他主机进行通信，需要配置至少两个网络设备。“lo”表示“local loopback”（本地回送），这是主机内部通信的虚拟设备。另一个是eth0，这是与NIC硬件对应的网络设备。

如果在这个阶段出现了问题，可以使用命令ifconfig，再次对设备进行配置。

```
# ifconfig eth0 192.168.0.10 broadcast 192.168.0.255 netmask 255.255.255.0
```

3．使用命令netstat，检查是否已经正确地配置了路由表。

```
# netstat -rn
Kernel IP routing table
Destination    Gateway       Genmask         Flags  MSS    Window  irtt  Iface
192.168.1.0    0.0.0.0       255.255.255.0   U      1500   0       0     eth0
0.0.0.0        192.168.1.1   0.0.0.0         UG     1500   0       0     eth0
```

在同一网络上，必须为“lo”和“eth0”设置网络地址。而且，你还必须设置网关地址，以建立与其他网络的通信。

如果路由表的配置不正确，可以使用route命令，再次配置路由表。

```
# route add -net 192.168.1.0
# route add default gw 192.168.1.1
```

4．使用ping命令，检查是否能与其他主机进行通信。

```
# ping 192.168.1.2
64 bytes from 192.168.1.2: icmp_seq=0 ttl=64 time=0.9 ms
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=0.5 ms
…
# ping 192.168.2.3
64 bytes from 192.168.2.3: icmp_seq=- ttl=64 time=0.9 ms
64 bytes from 192.168.2.3: icmp_seq=1 ttl=64 time=0.9 ms
…
```

如果在这一阶段出现了问题，可能的原因很多。首先，应检查网络电缆、网络接口和路由表。请确保网络电缆已经正确连接，而且网络设备（如网络集线器）正常工作。

5．使用命令nslookup，检查是否正确引用了域名服务器。

```
# nslookup
Default Server: dns.calleprivada.com.cn
Address: 192.168.10.2
```

>

如果在这一阶段出现了问题，请检查是否已将正确的 IP **地址写到了文件**/etc/resolv.conf **中。如果您对这些原理不太感兴趣您可以使用** Turbolinux **配置工具进行网络配置**,**命令是** netcfg**。**

第三章　TURBOLINUX 服务器安全

网络安全是一个关系国家安全和主权、社会的稳定、民族文化的继承和发扬的重要问题。其重要性，正随着全球信息化步伐的加快而变到越来越重要。“ 家门就是国门 ”, 安全问题刻不容缓。

网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

网络安全从其本质上来讲就是网络上的信息安全。从广义来说，凡是涉及到网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。

网络安全的具体含义会随着“ 角度 ”的变化而变化。比如：从用户（个人、企业等）的角度来说，他们希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护，避免其他人或对手利用窃听、冒充、篡改、抵赖等手段侵犯用户的利益和隐，同时也避免其它用户的非授权访问和破坏。

从网络运行和管理者角度说，他们希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现“ 陷门 ”、病毒、非法存取、拒绝服务和网络资源非法占用和非法控制等威胁，制止和防御网络黑客的攻击。

对安全保密部门来说，他们希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免机要信息泄露，避免对社会产生危害，对国家造成巨大损失。

从社会教育和意识形态角度来讲，网络上不健康的内容，会对社会的稳定和人类的发展造成阻碍，必须对其进行控制。

近来网络技术取得迅猛进展及用户数量急剧增加，Internet 迅速发展,Linux 随之成为最重要的网络操作系统中的一员,因此，Linux 环境下的安全问题也不能忽视。

Linux 与其它的 UNIX 派生物一样，内嵌 Internet 技术支持的操作系统。Linux 的特点之一就是灵活性，对安全而言，这既给用户带来好处也能带来灾难。如果是知识渊博的管理员,运行 Linux，就达到很高的安全性.如果不是,请不要随便改变没有把握的设置,这样也会尽量保证系统的安全.

Turbolinux 的最大好处是源码公开,不可能存在后门.

本章将介绍安全方面的基本知识，这些知识用户应该知道并且能够理解相关概念。

3.1 什么是安全？

对计算机系统和网络而言，安全主要是指采取措施防止非授权访问存储在各个计算机上或在各个计算机之间传输的数据。为了维护数据的完整，也为了防止数据被恶意删除修改，采取这些措施是绝对必要的。这一节讨论以下主题，以阐明和理解安全概念：

- 家庭安全
- 计算机安全
- Turbolinux 安全

3.1.1 家庭安全

当提及系统安全，诸如防火墙，加密，安全漏洞以及非授权访问等词汇马上就出现在人们的脑海中。

但这仅仅是方法。最重要的问题是“你想保护什么？”

暂且不提计算机，网络以及其他技术术语，考虑考虑发生在我们周围的事情。

例如，你为什么要锁门？原因大概不会是“因为我有钥匙”。你锁门是因为您不希望家里的物品被别人不经同意就拿走，不希望他们被损坏,不希望自己受到伤害.

我们按照以下思路考虑家庭安全：

- 关注的对象： 人及家里的财物
- 威胁： 火灾，闯入，行窃，欺骗
- 措施： 锁，警报，监视器，老鼠药

汇集了这些设施，你就能够开始谈论你的策略。

对于上锁，你能够想到的情况包括:家里无人;只有孩子在家的时候;夜晚。

你的策略就是应用最适合于你的情况的措施，无论它是什么措施。

在考虑安全策略时，容易犯的常见错误之一就是认为“大的应该包括小的”。

谁会花一千元来保护一个仅值一百元的表呢？这种过度的方法不仅会浪费你的金钱和精力，而且实际上还会消弱你的安全。例如，每次取下表和再带上时，都不得不打开保险箱。最终会变得厌烦懒惰，完全忘记锁保险箱。遵循以下方针是明智之举：

· 投资额不要大于你的物品的价值

· 不要盲目地牺牲便利

记住了这些要点，你的房子现在就安全了。但是仍然不能松懈。锁可能会被用坏和撬开，你也可能会把钥匙丢了。

安全需要具备不断的警惕性。必须定期重新评估策略的有效性，根据新的需要作相应的变化，甚至重新定义你想要保护的是什么。

3.1.2 计算机安全

计算机安全就像家庭安全一样，也是日常关心的事情。大多数的家庭安全都是共同的，不必详细地系统考虑。而对计算机来说，由于行业术语和技术问题，获得单一，一致的响应是不可能的。因此，根据实际情况阐明公司，学校以及其他组织机构的安全协议是非常重要的。这些协议将成为这些组织机构的安全策略。在制订安全策略时，应该特别注意以下事项：

- 对象，威胁，措施
- 职责和权限
- 法律
- 安全策略

对象，威胁和措施

对象分两大类：数据和计算机资源。

有不同的方法区分威胁。例如，做某件事是否是故意的，是属于物质上的还是属于知识方面的。

措施的建立应该不需要大量的具体的技术细节。

职责和权限

从技术的角度来看，有各种日常操作，例如建立或删除帐户，或诸如登录监视等特殊任务。应该清晰地鉴定整个操作以及职责范围的权限。

法律

阅读他人邮件，检查日志文件，以及其他活动可能会侵犯隐私。应该清晰地鉴定什么属于合法备份以及什么是属于为防止合法的侵犯而采取的控制。

安全策略

事先确定将如何管理安全策略，以及都有那些职责。安全策略是一种协议。它应该反映组织机构中和周围每个用户的的普遍情况。应该代表所有相关方的一致性。虽然没有包罗万象的完美安全策略，但是应该设法努力使它尽可能全面和广泛。

3.1.3 Linux 安全

因为 Linux 是从 UNIX 中派生出来的，为 UNIX 开发的安全概念和技术能够应用到 Linux 中。本节着重介绍 Linux 的特性。

- 二进制版本
- PC
- 开放式资源
- 用户的大量增加

二进制版本

Linux 版本中的大多数程序，包括免费软件，都是以编译好的二进制格式发布的。所以如果发现软件有安全问题，需要进行修复，然后再将新二进制软件发布给客户，在这段时间内客户的安全就会受到影响。而且由于单一的二进制是重新发布的，也有可能会出现新的问题以及新的安全漏洞，这对服务器的安全不利。

PC

在安装 Linux 的机器中，最常见的就是 PC。尽管硬件的可靠性各不相同，但是可以肯定的是,普通的计算机尤其易于被直接接触。PC 能够被打开，硬盘可以被拿出来，或者整台计算机会被偷走。有必要开始时就小心选择硬件设备，例如为服务器买一个固定用的装配支架。

开放式资源

有些人认为如果源代码对公众公开，安全漏洞就易于被利用。这种观点正确吗？事实是近来发现的已经成为严重问题的安全漏洞，与开放式资源无关。

实际上，正是由于资源是开放的，安全漏洞往往能够被迅速发现，世界各地的程序员和系统管理员能够很快为漏洞提供补丁程序，所以向公共开放资源能够看成是有利条件,并且,用户自己修复安全漏洞也是完全可能的.相反,如果不公开源码漏洞的发现具有偶然性,更多的是未发现的漏洞.及时发现漏洞也只能等待补丁,并且谁能保证这些系统中没有留有后门?

用户的大量增加

Linux 用户的数目和种类不断增加。随着类别的增加，维持广泛全面的安全战略变得愈来愈困难。随着用户数目的增加，心怀恶意的人的可能性增大。

3.2 Turbolinux 7 DataServer 的安全策略

Turbolinux 7 DataServer 是一个开始就被当作服务器运行的系统。服务器一词意味着很多不同种类的服务集合在一起，例如邮件服务，文件服务，名称服务，数据库服务等等。而且，因为它是 Linux，所以也能当作工作站。一旦确定了服务器的类型（根据它的目的），就能够检查相应的安全策略。

正如以前介绍的，安全策略必须反映给定组织机构以及周围每个用户的普遍情况。通过理解 Turbolinux 7 DataServer 潜在的策略，就能够创建一个相对简单和安全的系统。

尽管 Turbolinux 7 DataServer 的安装设计策略超出了本指南的范围，但是本节将介绍与安全直接相关的最重要的方面，以及频繁询问的问题。

3.2.1 “全部拒绝”方法

能够使用两种方法来建立安全策略：“全部拒绝”和“全部允许”。“全部拒绝”开始时是拒绝所有的，然后再选择性地允许所需要的。“全部允许”的观点是允许所有的通过，然后再选择性地拒绝不需要的。一般来说，“全部拒绝”更安全，而“全部允许”更简单。

如果在安装时选择“高安全”选项，Turbolinux 7 DataServer就采取“全部拒绝”方式。这种配置方式将停止所有由 **xinetd** 启动的服务，拒绝本机以外的所有访问。

3.1.2.1 帐户

帐户管理负责增加和删除帐户、设置有效期限等规则。同时,它也设置诸如密码加密格式和登录格式等。在 Turbolinux 7 DataServer 中，通常使用 shadow 密码,加密的密码内容并不存放在/etc/passwd，而是在/etc/shadow 文件中,该文件只能 root 用户读取,进一步加强了系统安全.通过使用 Linux-PAM（Linux 可插入鉴定模块）就可以安全方便的读取使用这些加密信息。有关 PAM 的详情，请参阅 **pam** 的 man page。

在 Turbolinux 中，没有设置密码失效时间的标准。全面的标准看来效果不好，因为这些设置都直接依赖于每个组织机构特定的规则。用 **chage** 命令能够更改这些设置。有关它们的详情，请参阅 **chage(1)** 的 man page。

注册过多的帐户信息可能会侵犯用户的隐私。Turbolinux 的标准帐户注册只在标准登录策略范围之内。

accton 命令设置进程账户控制。详情请参阅**accton(8)** 的 man page。

3.2.2 日志文件

对任何安全策略来说，设置日志文件的保持时间是重要的。Turbolinux 7 DataServer 设置日志文件每个星期循环一次，并保持前 4 次的文件（共 5 个星期）。此外，登录记录 *wtmp*，每个月循环一次，并保持上一次的记录（共 2 个月）。有关详情，请参阅 **logrotate(8)** 的 man page。

3.2.3 超级用户(root)权限和许可

超级用户(root)登录局限于控制台。不允许通过 **telnet** 或 (**ss**h) 以超级用户(root)直接远程登录。请参阅 **securetty(5)** 的 man page，了解如何从指定的终端，如串行控制台(**tt**y)，进行登录。

要想解除所有的登录限制，请将位于 */etc/pam.d/logi*n 中开始处的注释标识删除。

3.2.4 升级

升级软件可以增加新功能、提高性能、修复故障。在更新软件前，首先要确定是否确实需要升级；如果有必要，升级的最佳方法是什么？特别要注意通过网络传送来的软件包的内容。一定要确认该软件包没有“特洛伊木马”等病毒。

同时,如果有软件包文件的校验和(**MD**5)信息，请在安装下载文件前，用 **md5sum** 命令查看其准确性。

有关升级 Turbolinux 的信息在：

http://www.Turbolinux.com/support and *http://www.Turbolinux.com/security*

3.3 有关安全方面的机构组织的详情

这一节列出有关安全方面的各种机构组织的清单。注意，清单中可能会有遗漏。

非授权访问事件被称为“计算机安全事件”。如果发生此类事件，可以向“计算机安全事件响应组(CSIRT)”咨询信息和征求建议。计算机安全事件响应组的全球服务网址为：

http://www.csirt.ws/

CERT/CC 发布的 CERT 报告是安全方面的最权威的信息来源。CSIRTs 是针对特定的国家，地区或组织。属于此类的还有 CIAC (www.ciac.llnl.gov)，CERTCC-KR (www.certcc.org.kr), 以及 AUSCERT (www.auscert.org.au)。

安全方面的 Web站点	介绍
http://www.first.org/	FIRST 是世界各地的 CSIRTs 论坛。它的目的是 CSIRT 组之间共享信息，促进安全事件方面的合作。
http://www.rfc-editor.org/	很多 RFCs（请求注解）文件处理安全问题。RFC 2196（站点安全手册）和 RFC 2504（用户安全手册）对帮助创建安全的计算环境尤其重要。
http://www.w3.org/Security/Faq/www-security-faq.html	World Wide Web 安全常问问题
http://www.netscape.com/products/security/resources/notes.html	这个站点上有 Netscape 的安全注释，以及对 Netscape 和 JavaScript 中安全漏洞的修补程序

3.4 Linux 上的安全工具

Linux 上的安全工具有很多种类可供选用，例如 tcpdump 可以用来捕捉网络报文，通过分析这些报文可以分析网络安全问题；iptables 可以用来限制某些地址对服务器的指定端口的访问；Snort 是一个轻量级的网络入侵检测系统，可以用来检测出恶意的网络攻击行为。

3.4.1 snort 的特点和使用方法

网络入侵检测系统英文全称是 Network Intrusion Detection System，简称 NIDS，是目前

网络安全防范中最常用的工具之一，遵循“预防为主”的原则。Snort 是一个轻量级的 NIDS。它是一个基于 libpcap 包的网络监控软件，可以作为十分有效的网络入侵监测系统，可用于监测多种网络探测和攻击，例如：端口扫描、SMB 探测、OS 指纹特征检测（如用 nmap)、缓冲器溢出攻击、CGI 攻击、病毒攻击（如 CodeRed）等等。Snort 具有实时的报警能力，可将报警记入一个指定的文件——系统日志，或者将报警信息转发给指定的另一台机器上。对于管理员来说，要对系统日志进行经常性的、定时的检查是完全有必要的。

默认情况下 snort 是安装在系统上的，可以通过命令 rpm –qi snort 来查询。如果没有安装，请从 Turbolinux 安装盘上安装。

Snort 的启动：

默认情况下，snort 是不启动的，因此需要您手工启动。启动的方法是执行以下命令：

/etc/rc.d/init.d/snortd start

来激活 snort。如果要停止 snort 的运行，请执行命令：/etc/rc.d/init.d/snortd stop

如果希望 snort 每次系统启动后都能够自动启动，请执行如下命令：

chkconfig - -add snortd

可将 snortd 加入默认启动的系统服务列表中。如果要取消，请执行命令：

chkconfig - -del snortd

可将 snortd 从默认启动的系统服务列表中删除掉。

Snort 的使用：

启动 Snort 之后，所有的 snort 事件记录都放在/var/log/snort/目录下面。其中 alert 文件是示警文件，是对异常事件的报告。而 portscan.log 则是针对端口扫描的记录。通过查看这个目录下面的文件，就能够发现网络上对于服务器的网络探测行为。管理员可以根据这些日志进行分析判断并采取相应的措施。譬如发现来自某个地址的人员进行了多次端口扫描，那么可以推测该人企图恶意攻击系统。此时我们可以通过 ipchains 来封禁来自该地址对于本主机服务器指定和全部端口服务的访问。

Snort 的配置文件和规则：

Snort 的配置文件和规则集文件都位于目录/etc/snort/下。/etc/snort/snort.conf 是 snort 的配置文件，以*.rules 结尾的文件则是应用于 snort 检测系统的规则集文件。通过定义规则集，snort 可以探测到指定的行为。从某种程度上来说，规则集对于 snort 检测系统的作用就如同病毒库之于防杀毒软件一样。

Snort 的其他信息：Snort 的官方地址是：http://www.snort.org。关于 snort 的最新版本和最新的规则集以及更为详细的使用方法，均可以访问该站点来获得。

3.4.2 防火墙和 IPTABLES 的使用

3.2.4.1 防火墙技术

防火墙技术是建立在现代通信网络技术和信息安全技术基础上的应用性安全技术，越来

越多地应用于专用网络与公用网络的互联环境之中，尤以 Internet 网络为最甚。因特网防火墙是这样的（一组）系统，它能增强机构内部网络的安全性，因特网防火墙用于加强网络间的访问控制，防止外部用户非法使用内部网的资源，保护内部网络的设备不被破坏，防止内部网络的敏感数据被窃取。防火墙系统决定了哪些内部服务可以被外界访问；外界的哪些人可以访问内部的哪些可以访问的服务，以及哪些外部服务可以被内部人员访问。要使一个防火墙有效，所有来自和去往因特网的信息都必须经过防火墙，接受防火墙的检查。防火墙必须只允许授权的数据通过，并且防火墙本身也必须能够免于渗透。防火墙系统一旦被攻击者突破或迂回，就不能提供任何保护了。

3.2.4.2 Turbolinux 的防火墙

防火墙是提供网络安全性的重要手段之一，Linux 在内核中实现了包过滤型防火墙。包过滤就是查看所流经封包之表头(header)，并同设定的过滤规则作比较，由此决定整个封包的命运。它或许会决定 丢弃(DROP) 这个封包(例如，忽略它就如根本没收到它一样)，或是接收(ACCEPT)这个封包(例如，让这个封包通过)，或是其它更复杂的动作。包过滤型防火墙工作于网络层，它只能基于每个 IP 包或 TCP 包的特征(源地址，目的地址，TCP 连接的端口等)来匹配过滤规则。而其它专用的防火墙软件， 工作于应用层，除了包过滤外，有更强的功能。

首先让我们看一下服务器/客户机的交互原理。服务器提供某特定功能的服务总是由特定的后台程序提供的。在 TCP/IP 网络中，常常把这个特定的服务绑定到特定的 TCP 或 UDP 端口。之后，该后台程序就不断地监听（ listen)该端口，一旦接收到符合条件的客户端请求，该服务进行 TCP 握手后就同客户端建立一个连接，响应客户请求。与此同时，再产生一个该绑定的拷贝，继续监听客户端的请求。

举一个具体的例子：假设网络中有一台服务器 A（IP 地址为 192.168.98.1）提供 WWW 服务，另有客户机 B(192.168.98.100)、C(192.168.98.101)。首先，服务器 A 运行提供 WWW 服务的后台程序（比如 Apache）并且把该服务绑定到端口 80，也就是说，在端口 80 进行监听。当 B 发起一个连接请求时, B 将打开一个大于 1024 的连接端口(1024 内为已定义端口), 假设为 1037。A 在接收到请求后，用 80 端口与 B 建立连接以响应 B 的请求，同时产生一个 80 端口绑定的拷贝，继续监听客户端的请求。假如 A 又接收到 C 的连接请求（设连接请求端口为 1071），则 A 在与 C 建立连接的同时又产生一个 80 端口绑定的拷贝继续监听客户端的请求。每个连接都是唯一的。

3.2.4.3 IPTABLES

在 2.4 Linux 内核中，IPTABLES 替代了 2.2 中的 IPCHAINS。Iptables 模块能够对输入、输出的 IP 包进行过滤和管理。Iptables 模块是 LINUX2.4 内核中的 Netfilter 框架的一个组成部分。Iptables 由两个子系统组成：内核模块和用户接口应用程序。对 iptables 的支持必需被编译进 LINUX 内核或者编译成一个可装卸的模块。然后，可以为不同的任务（如伪装、端口转发、包过滤等）选择安装其它一些组件。同 ipchains 一样，您可以根据在编译到内核和可装载模块之间进行选择。在 Turbolinux 中， 已做进内核中， 你只需直接增加规则。

一个防火墙规则指定包的格式和目标。当一个包进来时，核心使用 input 链来决定它的命运。如果它通过了，那么核心将决定下一步包该发往何处（这一步叫路由）。假如它是送往另一台机器的，核心就运用 forward 链。如果不匹配，进入目标值所指定的下一条链，那有可能是一条 user defined 链，或者是一个特定值：ACCEPT，DENY，REJECT，MASQ，REDIRECT，RETURN。

大多数情况下，在路由器或防火墙计算机中用 iptables 进行网络地址转换（Network Address Translation-NAT，也称为伪装 Masquerading)。通常，您不应在普通的主机或工作站上使用 iptables。

毫无疑问用户需要以 root 身份登录系统来使用 iptables 工具，以 root 身份登录进入系统以后，你也许首先希望查看当前防火墙系统中有哪些设置，通过命令"iptables -L"来察看当前设定的防火墙规则，若希望了解防火墙设置的查看详细信息，可以使用"iptables --list"命令来查看。

默认情况下，系统有三条规则链：INPUT、OUTPUT 和 FORWARD，所有规则链的策略都为 ACCEPT。也就是说在配置任何规则以前，系统是完全开放的。

若你希望将你的系统作为防火墙使用，那么你需要打开 IP 转发开关：

```
echo "1" > /proc/sys/net/ipv4/ip_forward
```

添加规则

如果没有任何规则，iptables 则不会产生任何效应，下面我们就向现存的规则链中添加一些规则。若你不希望别人通过 ping 工具来探测你的主机，你可以使用下面的规则来限定：

```
iptables -A INPUT -p icmp -j DROP
```

参数"-A INPUT"设定 iptables 在 INPUT 链后添加该规则，参数"-p icmp"指示该规则是施用于 icmp 协议，参数"-j DROP" 指示匹配该规则的数据报应该被丢弃。现在向该服务器发送的 ping 数据，该服务器将会丢弃这些数据，因此的不到响应。其中协议名"icmp"是和大小无关的，可以是"icmp"也可以是"ICMP"。

若需要删除该规则，使服务器响应 ping 命令，则使用下面命令：

```
iptables -D INPUT 1
```

"-D"参数指示 iptables 工具删除 INPUT 规则链中的第一条规则。若你的规则链中有多条规则，则该命令不会影响到规则。这时候你也许希望清除前面所有命令定义的规则而从头开始，可以使用命令：

```
iptables -F INPUT
```

该命令指示 iptables 清空 INPUT 规则链中的所有规则。

阻塞 telnet 连接

现在我们来尝试一个稍微复杂一些的例子。我们希望阻塞来自外部网络到服务器的 SSH 连接但是允许内部网络的 SSH 连接。为了防止用户的用户名和密码外泄，因此组织所有的连接外部网络的 telnet 连接。

首先在 INPUT 规则链中设置一条允许内部网络 ssh 连接服务器的规则：

iptables -A INPUT -s 198.168.0.0 -p tcp --destination-port ssh -j ACCEPT

参数"-s"指定该规则适用于哪些源地址的连接。"--destination-port"指定 TCP 连接端口。

下面的规则阻塞所有来自外部网络对内部服务器的 SSH 连接：

iptables -A INPUT -s ! 198.168.0.0 -p tcp --destination-port ssh -j DROP

该命令和上面的命令是几乎是同一条命令，除了它定义的是阻塞外部网络的 SSH 连接。若你希望在外部网络中能连接内部服务器则不要定义该规则。要使定义的规则发挥作用，定义规则的主机必需是路由器，所有的数据都经过该服务器才能实现控制，否则这些规则无法发挥作用。同时注意上面规则定义中"！"和后面网络地址之间必须有个空格。

最后，为了阻塞连向外部的 telnet 连接，向 OUTPUT 规则链添加如下规则：

iptables -A OUTPUT -p tcp --destination-port telnet -j DROP

这一次定义的规则是添加到 INPUT 链中。当该规则被定义，用户试图通过 telnet 链接出去时，将会被阻塞，用户将得不到响应。这可能会引起用户以为是目标服务器出现了问题，因此我们修改该规则，不丢弃 telnet 数据，而是拒绝该数据：

iptables -F OUTPUT
iptables -A OUTPUT -p tcp --destination-port telnet -j REJECT

清空 OUTPUT 链接以后，我们将使用一个类似的命令，只是规则目标动作变为"REJECT"。这时候用户 telnet 外部服务器时会得到链接被拒绝的错误。

若希望允许 telnet 链接内部服务器，则清空 OUTPUT 规则链然后重新设定规则：

iptables -A OUTPUT -p tcp --destination-port telnet -d 198.168.0.0 -j ACCEPT
iptables -A OUTPUT -p tcp --destination-port telnet -d ! 198.168.0.0 -j REJECT

你也许现在会施用"iptables -L"命令来查看当前定义的规则。

iptables 的基本使用方法，正如你所看到的那样 iptablesr 的用法同 IP chinas 基本相仿，但是它更强大和灵活。更详细的信息请看 MAN 手册面和 HOWTO 中的相应部分。

3.5 加密

TCP/IP 在设计上，对硬件故障处置是得力的，但其自身并未确立安全性措施。例如，即使 tcpdump 命令也可以轻而易举地盗听，它甚至还有专用的工具。 今后在网络上保护自己，将成为越来越重要的课题，它与系统管理者息息相关。 密码化可以说是安全性策略的重要项目之一。这里将说明各种具有代表性的加密程序。

3.5.1 ssh

所谓 ssh(Secure Shell)是强化安全远程登录方式。 至今为止，使用 rsh 和 telnet 进行登记时，所登录的 ID 和口令将按明文在网络中传播。 若是内部网还行，在因特网上，则盗听，纂改的危险性时刻存在。 由于 ssh 将整个通信内容加密，所以可以进行更安全的运用。

ssh 的版本有 1.x 系列和 2.x 系列。 最新的版本分别为 1.2.27 和 2.0.13. 1.2.23 之前的版本已发现了安全漏洞，所以若您使用的是 ssh 1.2.23 之前版本的话，我们建议您去升级。

ssh 在用于个人目的时，是公开的，但在用于商用目的时，则需要许可证。

ssh 正式地址:

http://www.ssh.org/

3.5.2 Open SSL

所谓 OpenSSL 是指安装了 SSL (Secure Sockets Layer)和国际标准的密码协议—TLS，具有高性能且坚固的工具箱。 此外，如名称所示的那样，它是开放源代码的，所以不论商用还是非商用，它是公开的。 因此，在商用上也可以安全地使用。 (此时有一点附加条件，详细情况请参阅程序所附的手册)。

现在，OpenSSL 工具箱提供了 Apache 方式的许可证。 它可以把 Apache 作为强化了安全性后的 HTTP 服务器来使用。

该许可证可以从以下正式地址下载。

OpenSSL 正式地址:

http://www.openssl.org/

Apache-SSL 正式地址:

http://www.apache-ssl.org/

3.5.3 PGP

所谓 PGP(Pretty Good Privacy)就是在 E-mail 上极其坚固的公开密钥程序。 它已成为事实上的标准。

现在，PGP 由 Network Assoiates 公司开发，销售，已有公开版，商用版等各种产品。国际版 PGP 免费软件的最新版是 5.5i(只有 Windows95/NT 和 MacOS)和 5.0i(其它环境)。PGP 版本众多，由于存在着相互间的兼容性问题，使用时请多加注意。

美国 Network Assoiates 公司的地址:

http://www.nai.com/

The International PGP Home Page:

http://www.pgpi.org/

PGP 国际版的主页：
http://ac3.aimcom.com.cn/~macpgp/index.html

3.6 CERT advisory

CERT Coordination Center(CERT/CC)是进行网络脆弱性调查，研究的机构。 CERT/CC 是为解决 1988 年发生的在 DARPA 上的 Internet 蠕虫问题而成立的对策小组，它已迎来了 10 周年。 CERT/CC 针对各种网络威胁发行了 advisory，vulnerability notes，annual 等报告。

还有其它一些象这样的紧急对应调查机构，但在这里我们以 CERT/CC 的 advisory 为范例，来考察一下如何确保网络上的安全。 过去的 advisory 问题虽然几乎都已解决，但通过回顾过去的事件是从什么问题上发生及发生过程，将有助于我们防犯于未然。

CERT/CC advisory 可以从 http://www.cert.org/advisories/中获取。 这里汇集了从 1997 年最初的 advisory 到 1999 年 7 月止所有的 advisory。

3.6.1 TCP/IP 网络自身的攻击

CA-97.28.Teardrop_Land

IP Denial-of-Service Attacks

这是称为 Teardop 和 Land 的在 TCP/IP 级别上的攻击。 因为这两个攻击掌握了经常使用的 TCP/IP 实际安装的薄弱环节。 在 Linux 操作系统中，核心程序 2.0.30 以后版本已能对付 Land，2.0.32 以后版本可以对付 Teardrop。 v2.0 以后的 Turbolinux 版本已没有问题。

CA-98.01 smurf

“smurf” IP Denial-of-Service Attacks

将伪装的 ICMP 软件包流传到 broad cast 上。 它是转播特定网络，使特定主机不能使用的攻击。 虽然 Turbolinux 的核心程序没有被转播，但它有可能成为受害者。

CA-97.22.bind

BIND - the Berkeley Internet Name Daemon

这是有关诈称主机名的问题。 这里所述的问题虽然已基本解决，但就 TCP/IP 而言，还有不能解决，或者极难解决的其它主机名诈称问题。 /etc/hosts 中写有重要通信对象的主机，所以不使用 DNS 大概也是一个手段。

这种攻击的对象并不是特定的 OS，与其可以说是 TCP/IP 网络本身。 路由器等器材的薄弱性，也往往引起问题。 对于类似此类的攻击，防火墙是有效的。

3.6.2 服务器程序问题

CA-97.04.talkd

Talkd Vuclnerability

CA-97.05.sendmail

MIME Conversion Buffer Overflow in Sendmail Versions 8.8.3 and 8.8.4

CA-97.06.rlogin-term

Vulnerability in rlogin/term

CA-97.08.innd

Topic 2: Second vulnerability related to INN - ucbmail

Topic 1: Vulnerability in innd

CA-97.09 imap

Vulnerability in IMAP and POP

CA-97.16.ftpd

ftpd Signal Handling Vulnerability

CAa-97.27.FTP_bounce

FTP Bounce

CA-98.03 ssh-agent

Vulneerability in ssh - agent

CA-98.05.bind_probems

Multipie Vulnerabilities in BIND

1. Inverse Query Buffer Overrun in BIND 4.9 and BIND 8 Releases
2. Denial-of-Service Vulnerabilies in BIND 4.9 and BIND 8 Releases
3. Denial-of-Service Vulnerabilities in BIND 8 Releases

CA-98.09 imapd

Buffer Overflow in Some Implementations of IMAP Servers

CA-98.12 mountd

Remotely Exploitable Buffer Overflow Vulnerability in mountd

CA-99-03-FTP-Buffer-Overflows

Remote buffer overflows in various FTP servers

这些多是服务器的编码问题。它通过利用缓冲区溢出，在没有帐户的情况下，从外部用同服务器程序相同的权限执行命令。

Turbolinux 3.0 以后的版本已解决了这里所述的问题。Turbolinux 2.0 需要将 imap 上升至 4.1final-2TL 。 无论什么版本, imap 都不能在缺省的状态下启动。

作为不同的问题有 CA-97.27.FTP_bounce 。 它是使用 FTP 的 bounce 功能, 从其它的 FTP 服务器访问特定的 FTP 服务器。 利用这种手段就可以通过原来的存取控制。 这个问题在 wu-ftpd 中是不曾有过的。

3.6.3 特定应用问题和有效集合的问题

CA-97.10.nls

Vulnerability in Natural Language Service

CAa-97.11.libxt

Vulnerability in libxt

CA-97.13. xlock

Vulnerability in xlock

CA-97.17.sperl

Vulnerability in suidperlAisperlAj

CA-97.18.at

CA-97.18.at

Vulnerability in the atAAilAjprogram

CA-97.19.bsdlp

1pr Buffer Overrum Vulnerability

CA-97.23.rdist

buffer Overflow problem in rdist

CA-99-08 buffer Overflow Vulnerability in rpc.cmsd

Systems running the Calender Manager Service daemon, often named rpc.cmsd

这些几乎是旧程序引起的问题，它是普通用户利用 suid **程序错误获取特权用户权限的问题。**

CA-97.23 **在** Turbolinux **中没有关系。这是因为该版本的** rdist **没有附加** suid **的缘故。**

也有人说在 UNIX **中基本上不需要** suid **。若有错误的** suid **程序存在的话，则其它的** UNIX **保护机构将变得毫无意义。希望使用正确的** suid **程序时，请参考相关的参考文献。**

CA-99-05 Vulnerability in statd exposes vulnerability in automountd

systems running older versions of rpc.statd and automountd

CA-99-05 **在** Turbolinux DataServer 1.0 **以后的版本中没有关系。其内容是** rpc.statd **内的程序在** NFS **客户和服务器间所引起的问题，和** automountd **内的程序自动地安装某特定类型系统文件这类问题。在新的版本中没有问题。**

3.6.4 由于外部的输入，客户所产生的问题

CA-97.20. javascript

JavaScript Vulnerability

这是浏览器的活动完全被黑客所能观察的问题。旧的 Netscape **中有过这个问题。** Java **似乎花费了很大的力气克服这个问题，以使危害不影响到计算机上。但是大程序很难说将来不会发生这个问题。**

CAa-97.14.metamail

Vulnerability in metamail

CA-98.10 mime_buffer_overflows

buffer overflow in MIME-aware Mail and News Clients

这是邮件客户启动程序时的问题。Turbolinux DataServer **虽然不含有** pine **，但是** Turbolinux 3.0 **以前的版本中** pine **还是有问题的。为了安全起见，最好不要使用这些版本。**

MUA **的问题是通过引进** MTA **水准的分离数据程序可以减轻危害时发生的。重要的服务器设备中最好不要安装处理** Netscape **和** mime **的邮件客户应用程序。**

3.6.5 Web 服务器，特别是 CGI 问题

CA-97.24.Count_cgi

Buffer Overrun Vulnerability in Count.cgi cgi-bin program

CA-97.25.CGI_metachar

Sanitizing User-Supplied Data in CGI Scripts

CA-98.07.nph-test-cgi_script

Vulnerability in the httpd nph-tesst_cgi script

虽然这些并不与 Turbolinux 有什么特别的关系。但执行 CGI 的 Web 服务器，需要明确策略。在许多 CGI 中，有必要限定输入。关于这些问题请参考 ftp://ftp.cert.oorg/pub/tech_metacharacters`等。关于 Web 服务器的经营方法请参考相关的资料。

3.6.6 Turbolinux 中不包括的个别程序问题

CA-97.01.flex_lm
Multi-platform unix FLEXlm Vulnerabilities
CAa-97.26.statd
Buffer Overrun Vulnerabilities in statdAilMAjProggram
CA-98.02 CDE
Vulnerabilities in CDE
CA-98.08 qpopper_vul
Buffer Overrun in some POP servers
CA-98.11 tooltalk
Vulnerabilities in tooltalk RPC Service

CA-97.01.flex_lm 属于通过抓住称为 FLEXlm 许可证服务器出错的机会，普通用户也能用系统帐户启动命令这一类问题。

FLEXlm 虽然同 Turbolinux 没有关系，但是即使是 Linux 也往往使用商用的许可证服务器。运行没有被充分地保证，或者没有源码的程序最好避免使之用于重要设备上的服务器中。

3.6.7 Linux 以外的特定系统中的问题

CA-97.02.hp_newgrp
HP-UX newgrp buffer Overrum Vulnerability
CA-97.03.csetup
Vulnerability in IRIX csetup
CA-97.12.webdist
Vulnerability in webdist.cgi
CA-97.15.sgi_login
Vulnerability in SGI login LOCKOUT
CA-97.21.sgi_buffer_overflow
SGI buffer Overflow Vulnerabilities
CA-98.04.win32.webServers
Microsoft windows-based web Servers unauthorized access-long file names
CA-98.06.nisd
buffer overflow in NIS+
CA-98.13.tcp-denial-of-service
Vulnerability in Certain TCP/IP Implementations
CA-99-04 Melissa Macro Virus

Machines with Microsoft Word 97 or Word 2000

CA-99-06 ExploreZip Trojan Horse Program

Machines running Windows 95, Windows 98, or Windows NT

CA-99-07 IIS Buffer Overflow

Machines running Microsoft Internet Information Server 4.0

CA-99-09 Array Servicccces default configuration

IRIX systems ruunning the Array Services daemon

它们与 Linux 无关。是有关称为 HP-UX， IRIX， Windows 操作的 advisory 。只要看一下安全性有关的邮件目录(bugtraq 等)，就可以发现重大的问题似乎多出现在与 WindowsNT 有关的程序上。

3.6.8 其它的问题

CA-98-7 PKCS

Vulnerability in Some Usages of PKCS#1

这是由于 SSL 实际安装的缺点引起的 SSL 对话被解读的问题。

CA-99-01-Trojan-Tcp-Wrappers

Trojan horse version of TCP Wrappers

CA-99-02-Trojan-horses

Trojan-horses

这两件是特洛伊木马病毒。是所改变的 TCP_Wrapper 和 util-linux 被安装在 anonymous FTP 地址上的问题。

由于 util-linux 是在版本升级之后不久设置的，所以有可能引起重大的问题。虽然 Linux 与此没有关系，但是 Microsoft Internet Explorer 假信息似乎传播过。若进行了这类升级的话，系统的重要文件将被改变。

特洛伊木马病毒在 cert advisory 中也曾有过 8 例，今后有可能还会定期地发生。有 PGP 签名时，通过进行验证可以确实可行地加以防止。

CA-99-10 Insecure Default Configuration on RaQ2 Servers

Cobalt Networks RaQ2 single rack unit Internet servers

这是 Cobalt 公司的 Cobalt Networks RaQ2 Servers 固有的问题。从 Cobalt 公司可以获得升级的数据。

3.7 PC 中特有的问题

Turbolinux DataServer 虽然在 PC 上运转，但由此有这种可能性，即路由系统文件”被盗窃”。这是因为用户从外部拿来软盘，从这里进行启动，从而在硬盘上安装了某一路由系统文件。

象这类问题，Linux 可以设置两个阶段来防范。

第一阶段把从硬盘以外的启动设置成不可能的状态。从 BIOS 开始设置，进而在 BIOS 上施加口令，使变更不可能设置。

第二阶段是在 lilo 上设置口令。因为若将通常的情况放置不管的话，用单用户模式也是可以启动的，所以启动时，必须可以使之要求口令。这可以用/etc/lilo.conf 来设置。加上 password= ~ 一行后再执行 lilo。由于规定在/etc/lilo.conf 中写入原本的口令，所以请按如下的方式变更成只能读写 root:

```
# chmod 600 /etc/lilo.conf
```

这样只有输入口令时，才能启动计算机。

3.8 其它的安全性问题

以上主要考察了外部的威胁，据统计，实际报告的重大损害中，大部分是由内部的人员所引起的。本指南中并未涉及计划立案，用户教育，物理性破坏的保护，盗难的预防，人事管理，电话线路的保护。

其它所说的计算机内重要问题有备份管理，故障收集，重要升级信息的收集等。

收集，管理，监视故障是重要的业务之一。监视工具中有 swatch。虽然故障基本上由称为 syslogd 的守护程序来管理一切，但可以使用该输出的 swatch 进行监视。例如，也可以抽取 BAD SU(普通用户要成为超级用户而失败的故障)用邮件向管理者传送其内容。

```
# /BAD SU/   echo,bell,([管理者的邮件地址])
```

按上述的方式记述设置文件。

以上简单地介绍了使用工具，但该设置需要充分地理解 syslogd 的 log 格式化。讨论引进的问题也是可以的，但是请充分地了解其优点和缺点，自己承担其后果后再使用。

申请地址: ftp://ftp.stanford.edu/general/security-tools/swatch/

Turbolinux 有关的升级信息也可以从 Turbolinux China 的通告邮件目录

tlc-announce@turbolinux.com.cn 中获取。

构筑，管理服务器已成为非常重要的工作。通过处理 Linux 系统本身，使原来可以将责任转稼到某位人员身上而规定为由核心程序自我承担责任。就这个意义而言，高水平的工程师显得格外必要。这也可以说自由的文化赋予了培养高水平工程师的契机。

以下是参考文献，参考地址的 URL 一览表。

[Web Security Sourcebook]

Aviel Rubin,Daniel Geer and Marcus Ranum,John Wiley & Sons,Inc.,1997.

[CERT Cordination Center]

http://www.cert.org/

[FIRST]

http://www.first.org/

这些是与安全性相关的紧急对策小组的组织。

http://www.cs.purdue.edu/coast/

http://www.cs.purdue.edu/coast/archive/data/categ50.html

这是有关计算机安全的广泛项目和其归档文件。

[LinuxHelp Online]

http://www.linuxhelp.org/alerts.shtml

在这里收集了与 Linux 有关的 alert。

[The World Wide Web Security FAQ]

http://www.w3.org/Security/Faq/www-security-faq.html

这些是由 W3 consortium 引起的安全性 FAQ。

[Netscape Security Notes]

http://www.netscape.com/products/security/resources/notes.html

这些是 Netscape 公司的安全性记录。收集了 Netscape 和 JavaScript 的薄弱性及其解决方法等。

其它有关 TCP/IP 网络，UNIX，Linux 的事项，重要的是掌握基础知识。请加深对 OS 和网络基础知识的理解，这样在问题发生时，可以理解问题的所在。

3.9 补充：遇到问题时的对策

对于 Linux，若有不明白的时候，有以下几个调查办法。

- man 命令

这是有关命令使用方法和服务的联机手册。例如为调查”lilo”有关的内容，可执行以下的命令。

```
# man lilo
```

- /usr/doc

在/usr/doc 以下保存了各种各样的文件。特别是在/usr/doc/HOWTOJ 以下保存了日文文件。在缺省状态下，文件被压缩了，所以请在解压后充分地使用。

- 服务器构筑/使用指南

本指南说明了 Turbolinux 中文版的服务器构筑/使用方法。

- 一般书籍

现在，Turbolinux，Linux 总论，各类服务，PC-UNIX 等相关的专业书籍不断地上市。产品附带的用户基本指南中登载了参考文献一览表，所以请参考使用。

- TLC 地址

在 TLC 中，在以下的 URL 上公开了许多信息。

http://www.turbolinux.com.cn

在这里可以获得丰富的信息，如故障处理的 FAQ 和安全信息，用户库告示板和邮件目录等。

- TLC 支持

在 TLC 中，准备了安装支持(免费)，服务器支持包(有偿)等。详细情况请参照产品附带的支持指南

第四章　系统管理

对 Turbolinux 7 DataServer 的系统管理是通过设置各种配置文件、以及使用命令行来进行的。

- 此外，Turbolinux 7 DataServer 还提供了多种交互式配置程序，我们称之为 Turbotool（Turbo 工具），借助这些工具，可使很多系统管理任务大为简化。

使用这些工具可以用命令: setup 激活。

在本章中，首先介绍多种超级服务器、多种服务、以及多种端口监控程序。接下来，介绍了执行系统管理任务时你将用到的各种配置文件和命令，同时还给出了针对恰当的 Turbotool 的信息和屏幕截图。

超级服务器和服务器程序

在本节中，介绍了有关超级服务器的信息，并介绍了在 Turbolinux 中将它们组织在一起的方法。

这里的服务器概念不是指硬件,而是指为提供系统服务而运行的服务程序。

超级服务器

超级服务器负责控制普通服务器，超级服务器将根据需要启用、禁止或运行普通服务器。超级服务器也被称为 " Internet 超级服务器 " 或 " Internet 服务端口监控程序 "。

例如，根据需要定制某一超级服务器，该超级服务器即可对服务器程序（如 ftp、telnet 等）进行管理或控制。

其中，xinetd 就是超级服务器程序中的一种。

Turbolinux 提供了 serviceboard（turboservice），通过它，可帮助你控制自己的超级服务器。可以使用命令 turboservice,也可以通过命令 setup, 然后选择该功能。

服务器

Linux（或 UNIX）中很多可用的网络功能均能通过客户端程序和服务器程序之间的通信来实现，客户端程序运行在某一台计算机(客户机)上，服务器程序通常运行在另一台计算机（服务器）上，该服务器负责提供客户机所需要的功能。在客户机上负责发送请求并接受服务的程序称为客户端程序; 在服务器上接受请求并提供服务的程序称为服务器程序。例如，FTP 客户端程序会向服务器请求某些文件,而 FTP 服务端则响应这些请求并发送数据,当然这些过程必须是经过网络合法认证的。

端口监控程序

端口监控程序（daemon）是 UNIX 中的一个专业术语，用于表示服务器程序。这些程序会始终驻留在服务器机上并处于运行状态，在需要这些服务时，会调用它们提供相应服务。例

如，ftpd 和 telnetd 分别是针对客户端程序 ftp 和 telnet 的端口监控程序。对大多数端口监控程序而言，在它们的程序名称后面都带有字母“d”。

对于 Internet 来说，其诸多协议均有严格的定义，另一方面，它们的实施方式并没有预先确定下来。因此（例如），FTP 功能既能通过 ftp 来实施，也能通过 Proftp 实现。

超级服务器模式和独立模式

独立模式指直接启动服务器程序（端口监控程序），而无需某一超级服务器的管理或控制。当某一服务器程序（端口监控程序）是通过超级服务器启动(例如 xinetd)时，那么该服务器程序就被视为运行在“超级服务器模式”下。

超级服务器的功能和任务

下面介绍了超级服务器的功能、任务和优点。

减轻系统上的负载

在独立模式下启动的每一个服务器程序都必须驻留在内存中，这样，它们必然要占用相当多的内存。

如果采用超级服务器方式,这些服务仅在收到请求时启动，并在完成请求后返回待命状态，这样系统资源就不会被独占。

作为这些服务器程序的代理，处于不断运行状态的超级服务器仅会在需要时才运行它们，该超级服务器能减少对系统资源的需求并能降低系统的负载。

减轻系统管理方面的负担

对于在独立模式下启动（或停止）的每一个服务器程序来说，都需要对其单独的管理。这给系统管理员带来了更多的工作量，对于由每个服务器程序提供的多项服务来说，系统管理员必须单独处理其中的每一个。

通过使用超级服务器，就有可能在某一点上进行管理／控制。

- 提升系统的冗余性和坚固性

如果出于某种原因，运行在超级服务器模式下的某一特定的服务器程序不能正确执行其功能，但遇到下一个请求时，会重新启动,使其功能恢复正常。这就改善了系统的冗余性和稳定性。

目前，新的服务种类越来越多，这时就需要新的服务器程序，对这些程序进行单独管理正变得越来越不现实。

由于超级服务器能够对这些服务程序进行集中控制，这种能力使其成为系统管理不可或缺的工具。

事实上，在安装了超级服务器的 Linux 和 FreeBSD 中，大多数服务器程序均被配置为在超级服务器模式下启动。

4.1 超级服务器的不利方面

在下述情况下，每次收到请求时对服务器程序的启动和停止有可能增加系统上的实际负载。

- 存在需接受众多连接请求的多个服务时
- 某服务在启动初始化阶段和关闭阶段要占用太多资源时

这类服务使系统的负担加重，你可以通过使用独立模式来改善系统的效率。Web 服务器就是一个典型的例子，Web 服务器接收众多连接请求的可能性非常大；出于同样的原因，邮件服务器（Sendmail）也常常运行在独立模式下。因此，你应选择与任务相适合的模式。

4.1.1 Xinetd 超级服务器

Xinetd 就是最常见的超级服务器之一。

在 Turbolinux 7 DataServer 中，xinetd 是一个标准模块，它会在系统的引导过程中启动。

Xinetd 基础

在系统的引导阶段，将通过启动脚本/etc/rc.d/init.d/xinetd 来启动 xinetd。它将检查在配置文件中指定的端口，这些配置文件位于由文件/etc/xinetd.conf 给出的目录/etc/xinetd.d 中。然后，它将等待连接请求。当 xinetd 收到连接请求时，它将判断与端口相适应的服务，并将激活负责提供该服务的服务器程序,该服务是在该服务的子目录配置文件中设置的。在将连接请求提交给由 xinetd 启动的服务器程序后，将以标准输入、标准输出和标准错误方式启动服务套接字。当服务器程序完成任务后，xinetd 会再次检查这些端口。

端口监控程序	*/usr/sbin/xinetd*
配置文件目录	*/etc/xinetd.d/*
启动脚本	*/etc/rc.d/init.d/xinetd*
日志文件	*/var/lock/subsys/xinetd*
可用服务名称列表及端口号	*/etc/services*
协议名称和端口号码列表	*/etc/protocols*

Xinetd 服务配置文件

启动时，xinetd 程序会从一个文件中读取配置信息，默认情况下，该文件位于目录/etc/xinetd.d/下该服务的子目录中。配置文件中包含多个与变量有关的行。在行的开头包含字符“#”是注释行。每个配置文件均以少量注释行开始，在这些注释行中，详细介绍了服务名称、以及一些默认设置，后面跟着下述行：

service <name>（服务名称）	指明了服务的名称，如 ftp、telnet等。在文件/etc/services中记录了有效主机和端口的名称列表
Disable（禁止）	用于指明是否要由xinetd来管理该服务
socket_type	指明了套接字的类型，如stream（流式类型）、dgram（数据

（套接字类型）	报类型）等
Protocol （协议）	指明了所使用的协议类型，如tcp、udp等，这些类型从保存在文件/etc/protocols 内的有效协议列表中选择
Wait（等待）	用于表明wait（等待）或nowait（不等待）标志的标记。仅适用于dgram（数据报）套接字类型 Wait（等待）标志表明在执行请求／应答交换时，需要等待一段时间；nowait（不等待）标志表明请求不会等待应答
User（用户）	如“root”超级用户(root)和“nobody”用户，指明了用户在访问服务时的许可权限
Server（服务器）	给出了要执行的服务器程序的完整路径名称
Server_args (服务器参数）	服务器程序启动中指定的选项参数。

Xinetd 的安全策略

在 Turbolinux 中，高安全选项的默认值针对安全设置作了最优配置。关闭所有没有必要运行的可用的端口监控程序。将服务的 disable 参数设置为值 yes，禁止所有服务。

允许更改默认的 xinetd 设置（重新启动）

在目录/etc/xinetd.d/下对配置文件所作的更改和编辑，不会使新设置自动生效。要想让这些更改发挥作用，首先必须杀死“kill”当前正在运行的 xinetd，然后重新启动或重新加载 xinetd。可执行下述命令之一：

```
# killall -HUP xinetd
# /etc/rc.d/init.d/xinetd restart
```
或
```
# /etc/rc.d/init.d/xinetd reload
```

配置示例

在下面的示例中，给出了使用命令 telnet 设置服务许可时所需要的步骤。在该示例中，假设存在一个单独的客户端--主机连接，服务器主机的 IP 地址是 192.168.1.52，客户端的 IP 地址是 192.168.1.53，其中 telnet 用于提供许可功能。

1． 使用文本编辑器(如 vi)，打开文件/etc/xinetd.d/telnet，并找到下面这行内容：

```
disable = yes
```

2. 覆盖单词 yes，将其更改为 no：

```
disable = no
```

3. 输入下述命令，使更改生效：

```
# /etc/rc.d/init.d/xinetd restart
```

4． 在文件/etc/hosts.allow 的末端插入下行内容：

```
in.telnetd: 192.168.1.53
```

访问控制会自动查询文件/etc/host.allow 以确定服务许可情况。该行内容表明该主机已被

授予了使用 telnet 服务的许可。

关于访问控制的详细解释，请参阅后面的“访问控制”部分。

启动超级服务器脚本的命令行参数

启动脚本/etc/rc.d.init.d/inet 包含下述命令行参数：

/etc/rc.d/init.d/xinetd start	启动 xinetd
/etc/rc.d/init.d/xinetd stop	停止 xinetd
/etc/rc.d/init.d/xinetd status	显示 xinetd 的状态
/etc/rc.d/init.d/xinetd restart	重新启动 xinetd
/etc/rc.d/init.d/xinetd reload	重新加载 xinetd

重新启动“restart”和重新加载“reload”所执行的操作相同。

Xinetd 操作确认

Turbolinux 默认设置 xinetd 为运行。按下述方式使用命令 ps 可检查 xinetd 的状态：

```
ps ax | grep xinetd
400 ? S 15:20 0:00 xinetd
```

当 xinetd 正常运行时，会出现与上面相类似的信息。如果你未能见到上面所示的信息，那么或是因为 xinetd 的运行不正常，或是根本就没安装 xinetd。你可以使用命令 serviceboard 来证实 xinetd 是否正在运行。如果在 xinetd 条目上有“*”的标志，就表明它正在运行。

要想重新启动 xinetd，可键入下述命令：

```
/etc/rc.d/init.d/xinetd restart
```

4.1.2 访问控制

当 xinetd 收到来自客户端的请求时，也会将对服务的访问置于其控制之下。这类访问控制功能以前是由 TCP_Wrapper（或 tcpd）来管理的，但在目前，xinetd 也管理这些功能。当 xinetd 收到来自客户端的服务请求时，它将读取服务访问许可文件/etc/hosts.allow，以及访问禁止文件/etc/hosts.deny, /etc/hosts.allow 优先 /etc/hosts.deny。

文件/etc/hosts.allow 的格式如下：

[daemon_list] : [host_list] : [command]

其中：

[daemon_list]	端口监控程序,可以使用逗号将多个名称分隔开来。
[host_list]	主机名称或 IP 地址。可以使用逗号将多个名称分隔开来。还可以指定域和网络，或采用单独方式，或使用通配符。允许使用相同的域和网络名称。可以将所有这些名称组合在一个列表中。
[command]	与 [daemon_list]调用的服务器程序名不同，当运行 xinetd 命令时，可以指定其他服务程序的绝对路径名。

文件/etc/hosts.deny 的格式与上面所给出的文件/etc/hosts.allow 的格式完全相同。

在[host_list]后面，可跟随下述描述符：

ALL	与所有的主机匹配
LOCAL	与名称中不包含点符号“.”的主机匹配
UNKNOWN	与来自不明确或未知用户名或主机名的访问匹配
PARANOID	当主机名和 IP 地址不同时，匹配
EXCEPT	除了…以外
.domain	与主机名中包含.domain 的主机匹配（例如，ns.example1.com 是服务器 name.domainname，邮件服务器是 mail.example1.com）。
192.168.	与地址为 192.168.x.x 的主机匹配
192.168.0.0	225.225.255.240 对于带有子网掩码 255.255.255.240 的 IP 地址 192.168.0.0 来说，与位于地址范围 192.168.0.x 内的所有主机匹配，其中 x 的取值范围为 0～15。

xinetd 超级服务器会按下述顺序解释数据。

1． 如果在文件 hosts.allow 中允许主机访问，就会为该主机授予许可权限。
2． 如果在文件 hosts.deny 中禁止主机访问，就会禁止该主机的许可权限。
3． 如果未指明允许或禁止主机访问，那么就会为该主机授予许可权限。

示例

要想查看配置文件/etc/hosts.allow 中的默认设置，可键入下述命令。

```
# less /etc/hosts.allow
hosts.allow
# This file describes the names of hosts which
# are allowed to use the local INET services,
# as decided by the '/usr/sbin/tcpd' server.
#
ALL : 127.0.0.1 :
```

内容“ ALL:127.0.0.1:”表明该主机已被授予了访问所有服务的许可权限。

注意这里的 ALL 不是[host_list]域,是[daemon_list]域。意思是对本机开放所有的服务。

要想查看配置文件/etc/hosts.deny 中的默认设置，可键入下述命令。

```
# less /etc/hosts.deny
# hosts.deny
# This file lists the names of hosts which
# are *not* allowed to use the local INET services,
```

as decided by the '/usr/sbin/tcpd' server.

ALL : ALL

内容" ALL: ALL **"表明，对于未在文件**/etc/hosts.deny **中指出的所有程序来说，对它们的访问均将被禁止。这可为系统安全提供额外的保护措施。**

配置示例

没有必要更改文件/etc/hosts.deny **中的默认配置。对于文件**/etc/hosts.allow **来说，下面介绍了一些配置示例。**

在这样一种情形下，服务器的地址是 192.168.0.2**，而且系统管理员希望为地址为** 192.168.0.3 **的客户端授予使用所有服务的许可权限，可以进行如下设置。**

ALL: 192.168.0.3 : allow

对于主机 192.168.0.x**，授予** ftp **许可权限可对文件**/etc/hosts.allow **如下设置**:

in.proftpd: 192.168.0. : allow

4.2 安装和升级软件包

由于系统可能需要升级或增加新的功能

Turbolinux 采用了 RPM 作为其软件包管理器。它提供了一个有效的管理环境，在此环境中，可以安装、卸载、升级、或检查软件包。它还能对软件包之间存在的相关性进行管理。

无论你采用何种方式安装软件包，应清楚，某些软件包的安装要求具有超级用户的全县。软件包保存在 Turbolinux Install 光盘的 turbo/RPMS/目录下。

4.2.1 使用 rpm

可以按下述格式使用 rpm 命令：

$ rpm [options] [RPM package name]

常使用的选项参数有：

-I	安装
-U	升级
-e	删除
-h	用字符“ # ”显示进展状态
-v	显示详细信息（与-h 一起使用可获得更好的显示效果）
-q	查询当前已安装了哪些软件包

下面以软件包 sendmail-8.11.6-2.i586.rpm 为例讲解 rpm 命令的使用方法。

该软件包在 Turbolinux DataServer 第一张光盘的 /turbo/RPMS/ 目录下。

插入光盘,改变路径到该目录:

mount /mnt/cdrom

cd /mnt/cdrom/turbo/RPMS

安装软件包命令:

rpm -ivh sendmail-8.9.3-17.i386.rpm

升级软件包命令:

rpm -Uvh sendmail-8.9.3-17.i386.rpm

卸载软件包:

rpm -e sendmail

查看 RPM 软件包内容：

rpm -ql sendmail

RPM 帮助:

man rpm

4.2.2 使用 Turbopkg

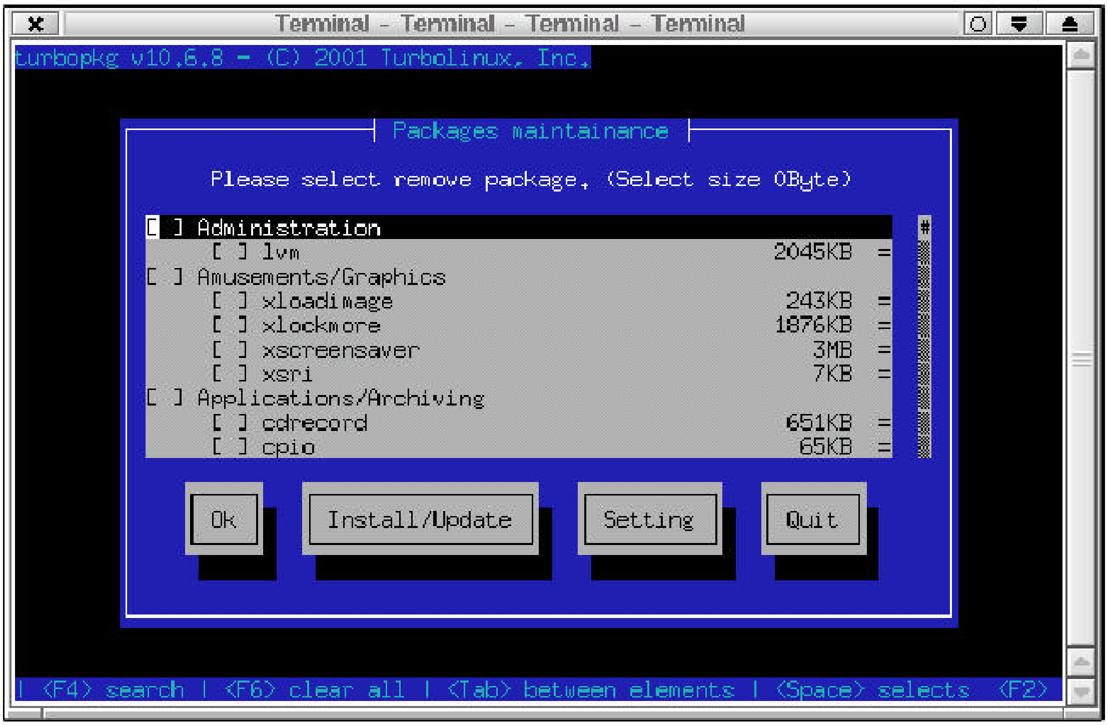
软件包管理器 turbopkg 是 RMP 软件包管理器的菜单化版本。使用它，你可以安装新的软件包，也可以删除以前安装的软件包。运行 turbopkg，键入下述命令：

turbopkg

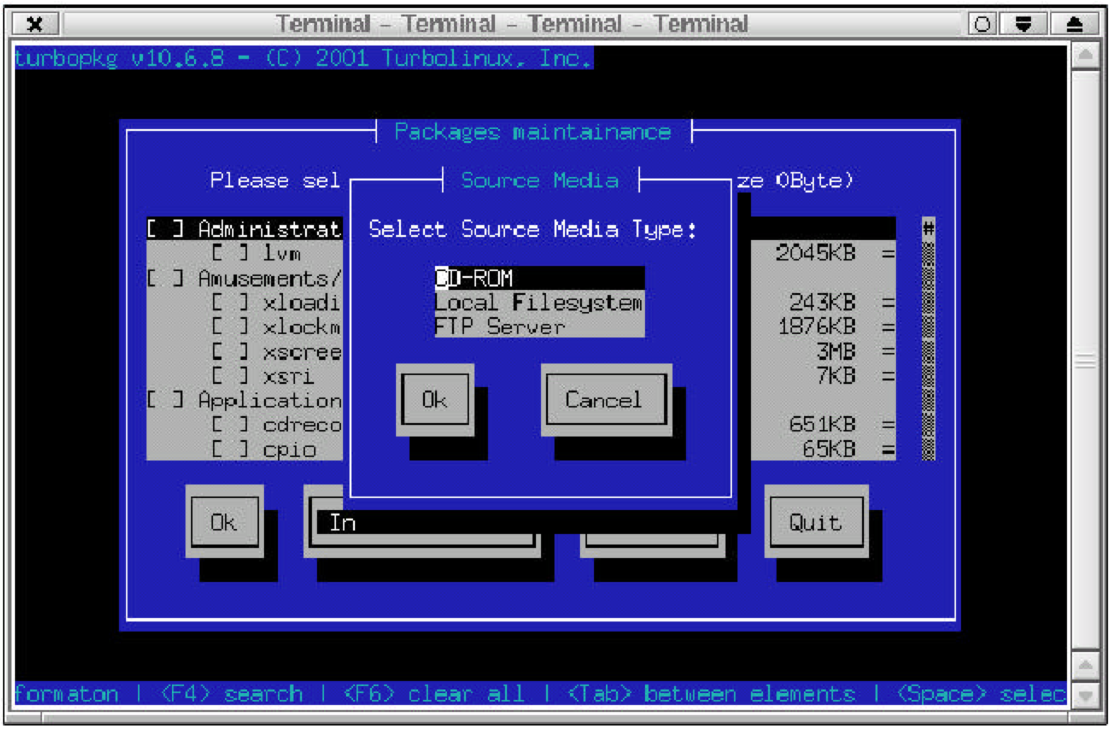
这时，将出现 turbopkg 欢迎屏幕,要想安装新的软件包或删除已存在的软件包，可：

1． 在 turbopkg 欢迎屏幕上选择“Maintenance”（维护）

这时，将出现软件包维护屏幕：



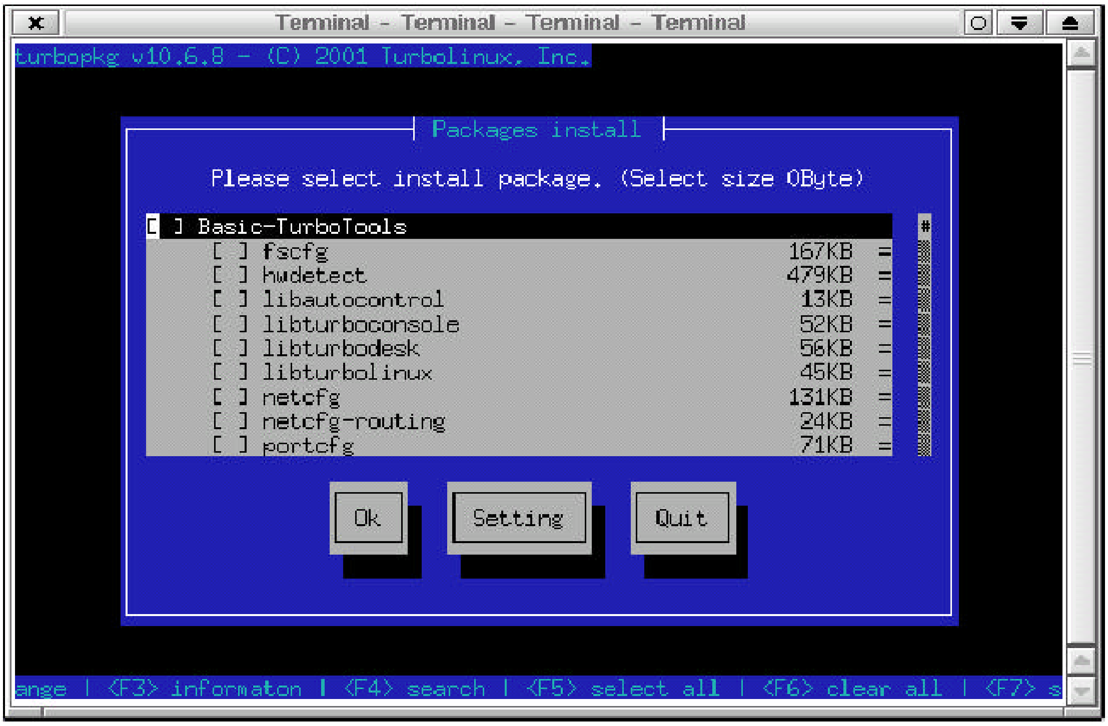
2． **选择“**Install/Update**”（安装／升级）选项，显示“**Source Media**”（源介质）屏幕，**



在源介质屏幕上，给出了三种选择，分别是：CD-ROM、Local Filesystem**（本地文件系统）、以及** FTP Server（FTP **服务器）。**

3． 选择打算安装的 RPM 软件包所在的源介质。

4． 选择 OK，显示软件包安装屏幕（请参见图 2-4)。



5． 亮选希望安装的软件包，按下空格键，选中新的软件包，或将以前选中的软件包选掉。

当你在某一组中选择了一个软件包时，组和软件包的复选框会发生变化，反映出下述内容：

组复选框表明：

*	选择了该组中所有的软件包
-	选择了该组中特定的软件包
None	未选择该组中的任何软件包

软件包复选框表明：

*	选择了希望安装或升级的软件包
R	选择了打算删除的软件包
None	未选择
X	软件包不存在

进行选择时，已选择软件包的总容量将显示在屏幕上方。

在定制“软件包安装”屏幕的最右一列中，会显示出下面所给出的标志之一

＋	当前安装的软件包
－	早期的软件包
＝	相同的软件包
None	新软件包
R	软件包将被删除

功能键指定了相应的功能：

F2	更改视图
F3	显示与所选软件包有关的信息
F4	查找软件包
F5	全部选择
F6	全部清除
F7	升级
F8	选择新软件包

4.3 服务

对于服务器的设置和操作，最重要的是要了解对服务进行控制的基本原理。关于每个服务的详细介绍，请参见相应的章节。在这里，仅从整个系统的角度，给出管理和配置任务的讲解。

启动脚本

服务启动脚本位于/etc/rc.d/init.d 下。

使用这些脚本，可以启动、停止、重新启动各项服务。

例如，你可以使用下述命令来重新启动 Samba 服务

```
# /etc/rc.d/init.d/smb restart
```

不同的启动脚本，参数选项会有所不同。在每个相应的启动脚本文件中，给出了详细的解释。

例如，/etc/rc.d/init.d/smb 包含的内容如下

```
. /etc/rd.d/init/d/functions
./etc/sysconfig/network
[ ${NETWORKING} = "no" ] && exit 0
[ -f /etc/smb.conf ] || exit 0
case "$1 in
start)
echo -n "Starting SMB services: "
daemon smvd -D
daemon nmdc -D
echo
touch /var/lock/subsys/smb
;;
stop)
echo -n "Shutting down SMB services: "
killproc smbd
killproc nmbd
rm -f /var/lock/subsys/smb
```

```
echo ""
;;
status)
status smbd
status nmbd
;;
restart)
echo -n "Restarting SMB services: "
$0 stop
$0 start
echo "done."
;;
*)
echo "Usage:smb{start|stop|restart|status}"
exit 1
esac
```

可以看出,除了“ start ”外，smb 还能接受通常的选项“ stop ”（停止）、“ restart ”（重新启动）、以及“ status ”（状态）。

运行级别

作为一种类 UNIX 系统，Linux 也具有“ run levels ”（运行级别）的功能，在引导过程中会显示出系统的状态。在表 2-1 中，给出了 Turbolinux 的设置情况。

表 2-1 运行级别

运行级别	描述	附加信息	目录
0	暂停	断电关机	*/etc/rc.d/rc0.d*
1	单用户模式		*/etc/rc.d/rc1.d*
2	多用户模式	禁止了 NFS	*/etc/rc.d/rc2.d*
3	多用户模式	默认（命令行方式登录）	*/etc/rc.d/rc3.d*
4	配置模式	记录安装配置	/etc/rc.d/rc4.d
5	多用户模式	默认（图形方式登录）	/etc/rc.d/rc5.d
6	重新引导	重新引导	/etc/rc.d/rc6.d

默认的运行级别是“ 3 ”。默认的运行级别记录在文件/etc/inittab 的第 1 行上，如下所示：

```
id:3:initdefault:
```

跟随在 id:后面的号码用于设置运行级别。对于本例，运行级别是“ 3 ”，即多用户模式下的命令行登录。如果你打算将登录方式更改为 “图形登录的多用户模式”，应将该号码更改为 5，保存/etc/inittab.下一次系统重新启动后将会图形方式登录.注意,如果您此时还没有经正确配置 X window 系统，屏幕将不停的闪烁试图进入图形模式,请确保正确设置 X window 系统.

运行级别“4”通常为空，允许 Linux 发布商设置他们自己的引导模式。

启动各运行级别

上页表 2-1 所示目录中的文件指明在每个运行级别下将启动哪些服务。针对每个运行级别，其目录中的大多数文件均是符号链接，这些符号链接指向目录/etc/rc.d/init.d 下的文件。下面给出了/etc/rc.d/rc3.d 的大部分内容：

```
ls -o /etc/rc.d/rc3.d

total 0

lrwxrwxrwx 1 root 16 Feb 26 2001 K08autofs -> ../init.d/autofs*
lrwxrwxrwx 1 root 7 Feb 26 2001 K10radiusd -> ../init.d/radiusd*
lrwxrwxrwx 1 root 19 Feb 26 2001 K14alsasound -> ../init.d/alsasound*
lrwxrwxrwx 1 root 17 Feb 26 2001 K15proftpd -> ../init.d/proftpd*
lrwxrwxrwx 1 root 13 Feb 26 2001 K20nfs -> ../init.d/nfs*
lrwxrwxrwx 1 root 19 Feb 26 2001 K34yppasswdd -> ../init.d/yppasswdd*
lrwxrwxrwx 1 root 15 Feb 26 2001 K35atalk -> ../init.d/atalk*
lrwxrwxrwx 1 root 13 Feb 26 2001 K35smb -> ../init.d/smb*
lrwxrwxrwx 1 root 15 Feb 26 2001 K41xntpd -> ../init.d/xntpd*
lrwxrwxrwx 1 root 13 Feb 26 2001 K60lpd -> ../init.d/lpd*
lrwxrwxrwx 1 root 18 Feb 26 2001 K60mars-nwe -> ../init.d/mars-nwe*
lrwxrwxrwx 1 root 16 Feb 26 2001 K65kadmin -> ../init.d/kadmin*
lrwxrwxrwx 1 root 15 Feb 26 2001 K65kprop -> ../init.d/kprop*
lrwxrwxrwx 1 root 16 Feb 26 2001 K65krb524 -> ../init.d/krb524*
lrwxrwxrwx 1 root 17 Feb 26 2001 K65krb5kdc -> ../init.d/krb5kdc*
lrwxrwxrwx 1 root 16 Feb 26 2001 K79identd -> ../init.d/identd*
lrwxrwxrwx 1 root 14 Feb 26 2001 K80nscd -> ../init.d/nscd*
lrwxrwxrwx 1 root 16 Feb 26 2001 K84ypserv -> ../init.d/ypserv*
lrwxrwxrwx 1 root 17 Feb 26 2001 K89portmap -> ../init.d/portmap*
lrwxrwxrwx 1 root 18 Feb 26 2001 K92iptables -> ../init.d/iptables*
lrwxrwxrwx 1 root 17 Feb 26 2001 S10network -> ../init.d/network*
lrwxrwxrwx 1 root 17 Feb 26 2001 S14nfslock -> ../init.d/nfslock*
lrwxrwxrwx 1 root 15 Feb 26 2001 S15nfsfs -> ../init.d/nfsfs*
lrwxrwxrwx 1 root 14 Feb 26 2001 S16apmd -> ../init.d/apmd*
lrwxrwxrwx 1 root 16 Feb 26 2001 S20random -> ../init.d/random*
lrwxrwxrwx 1 root 16 Feb 26 2001 S30syslog -> ../init.d/syslog*
lrwxrwxrwx 1 root 13 Feb 26 2001 S40atd -> ../init.d/atd*
lrwxrwxrwx 1 root 15 Feb 26 2001 S40crond -> ../init.d/crond*
lrwxrwxrwx 1 root 14 Feb 26 2001 S50inet -> ../init.d/inet*
lrwxrwxrwx 1 root 18 Feb 26 2001 S52synctime -> ../init.d/synctime*
lrwxrwxrwx 1 root 14 Feb 26 2001 S55sshd -> ../init.d/sshd*
```

lrwxrwxrwx 1 root 18 Feb 26 2001 S75keytable -> ../init.d/keytable*

lrwxrwxrwx 1 root 14 Feb 26 2001 S95innd -> ../init.d/innd*

lrwxrwxrwx 1 root 11 Feb 26 2001 S99local -> ../rc.local*

以“S”开头的文件名是在引导系统时依次启动的服务。以“K”开头的文件名是系统关闭时依次关闭的服务。

直接跟在“S”或“K”后的数字显示了使用该文件的顺序。如果直接更改了这些文件，要想使这些设置起作用，就必须创建遵循上述规则的符号链接文件。如果符号链接所指向的文件已被删除，将不能启动对应的服务。

更改运行级别

超级用户可以运行命令 init 更改正在运行的系统运行级。

例如，要想将运行在多用户模式下（运行级别“3”或“5”）的系统更改为单用户模式，可键入下述命令：

init 1

类似地，如果你执行了 init 0 或 init 6，其效果与执行命令 halt 或 reboot 相同。

当运行在单用户模式下时，其他用户不能使用该系统。命令 telinit 只会临时更改运行级别，不会将所作的更改写入文件/etc/inittab。

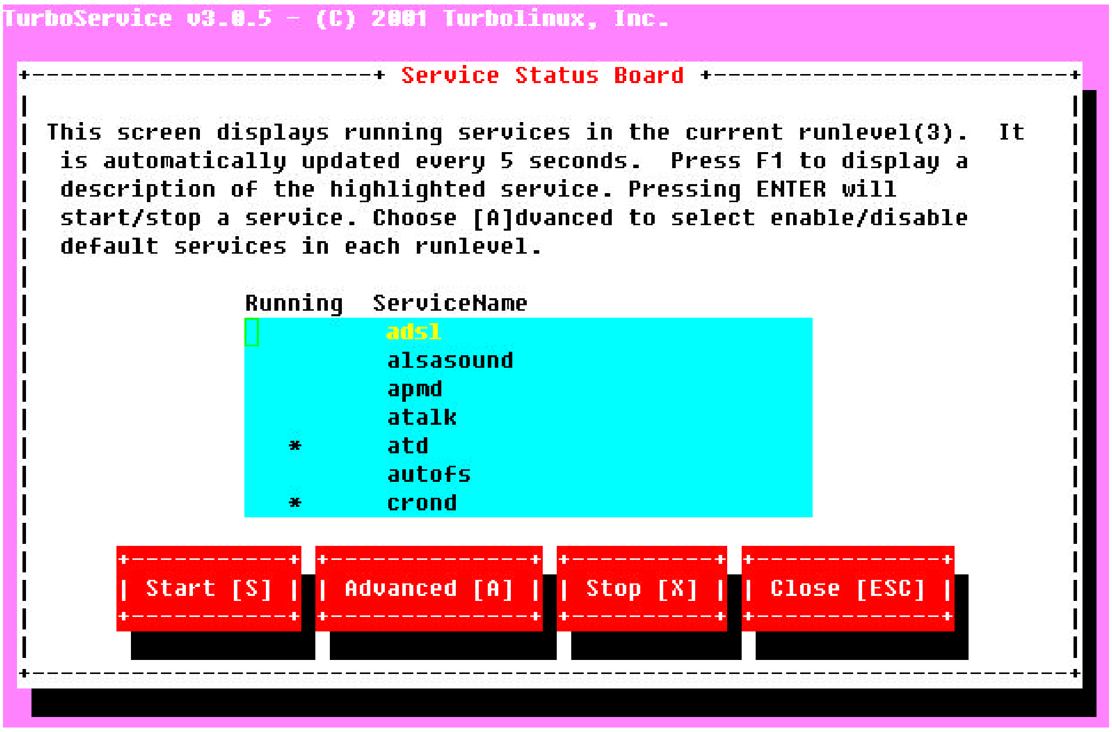
4.4 Serviceboard – turboservice

serviceboard (turboservice)工具管理 Turbolinux 的服务和端口监控程序。从命令行或使用 setup 选择该功能，你可以决定是否启动（或停止）某一服务。你还可以在引导系统时（或更改运行级别时）启动该工具。

执行下述命令即可启动 serviceboard：

serviceboard

这时，将出现服务配置屏幕，请参见图 2-5。



4.4.1 当前的运行级别状态

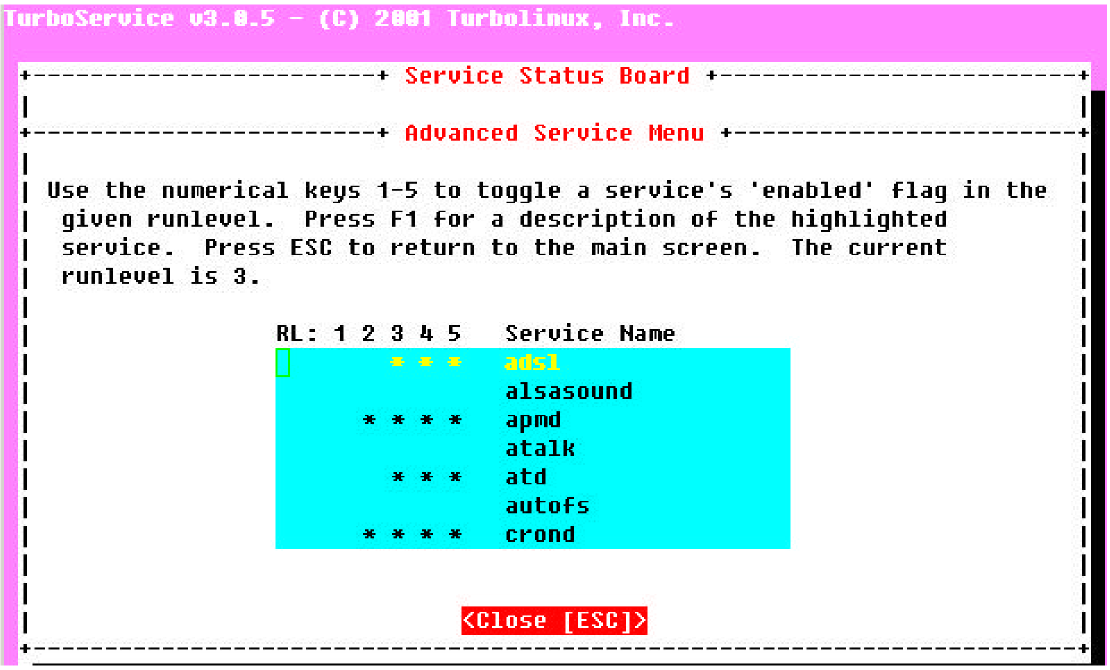
运行 serviceboard 时，在屏幕中央会显示一个列表框。它显示了在当前运行级别下，是否正在运行这些服务（下面会给出详细解释）。与这些服务对应的脚本位于目录/etc/rc.d/init.d/下。

[*]	服务正在运行
[ ]	服务已停止

使用 Enter 键，可对列表框中所选择的服务的运行状态进行切换。

设置当前的运行级别

在初始屏幕显示中，给出了当前的运行状态。若选取择 Advanced 显示为下图



在这里，你可按数字 1,2,3,4,5 **来设定相应运行级别时要启的服务。**

4.5 网络配置

配置或控制网络服务的文件很多。下面是 TCP/IP **网络所需的最低配置。**

文件/etc/rc.d/init.d/network

网络启动脚本文件称为“ network ”**，它位于目录**/etc/rc.d/init.d **下。**
使用下述命令即可启动“ network ”**文件。**

etc/rc.d/init.d/network start

除了“ start ”**（启动）外，文件**“ network ”**还能接受我们熟悉的选项**“ stop ”**、**“ restart ”**和**“ status ”**（状态）。**

文件/etc/sysconfig/network

在该文件中，记录了系统的网络设置情况（IP **地址、主机名、网关** IP **地址）。下面给出了一个文件示例：**

NETWORKING=yes
PROFILENAME="(null)"
HOSTNAME=jon.Turbolinux.us
GATEWAY=192.168.1.1
GATEWAYDEV=eth0
FORWARD_IPV4=no
IPX=no
TIMESERVERATBOOT=no
TIMESERVERTYPE=ntp
TIMESERVERHOST=(none)
TIMESERVERRESYNC=(none)

文件/etc/sysconfig/network-scripts/ifcfg-[dev_name]

该文件记录了连接到系统的网络接口的设置情况。标签[dev_name]**对应的是已连接网络接口的设备名称。**[dev_name] **为** eth0,**不是第一块网卡**; **为** eth1,**不是第二块网卡**.

该设备的 IP **地址和网络掩码分别记录在各自的配置文件中。**
下面给出了这类文件的一个示例(/etc/sysconfig/network-scripts/ifcfg-eth0):

```
DEVICE=eth0
IPADDR=192.168.1.82
NETMASK=255.255.255.0
NETWORK=192.168.1.0
BROADCAST=192.168.1.255
ONBOOT=yes
BOOTPROTO=none
```

文件/etc/resolv.conf

系统的域名、系统所使用的 DNS **解析服务器的** IP **地址均记录在文件**/etc/resolv.conf.
下面给出了这类文件的一个示例：

```
domain Turbolinux.us
search Turbolinux.us
nameserver 192.168.1.2
nameserver 210.255.54.18
```

文件/etc/HOSTNAME

该文件记录本系统的主机名称:

jon.Turbolinux.us

文件/etc/hosts

该文件记录每个主机的 IP **地址以及对应的主机名称，每个占一行。该文件也用于本地主机的域名解析**.

下面给出了这类文件的一个示例：

```
127.0.0.1       localhost.localdomain localhost

192.168.1.82       jon.Turbolinux.us jon
```

检查或设置网络接口的状态您可以使用命令:

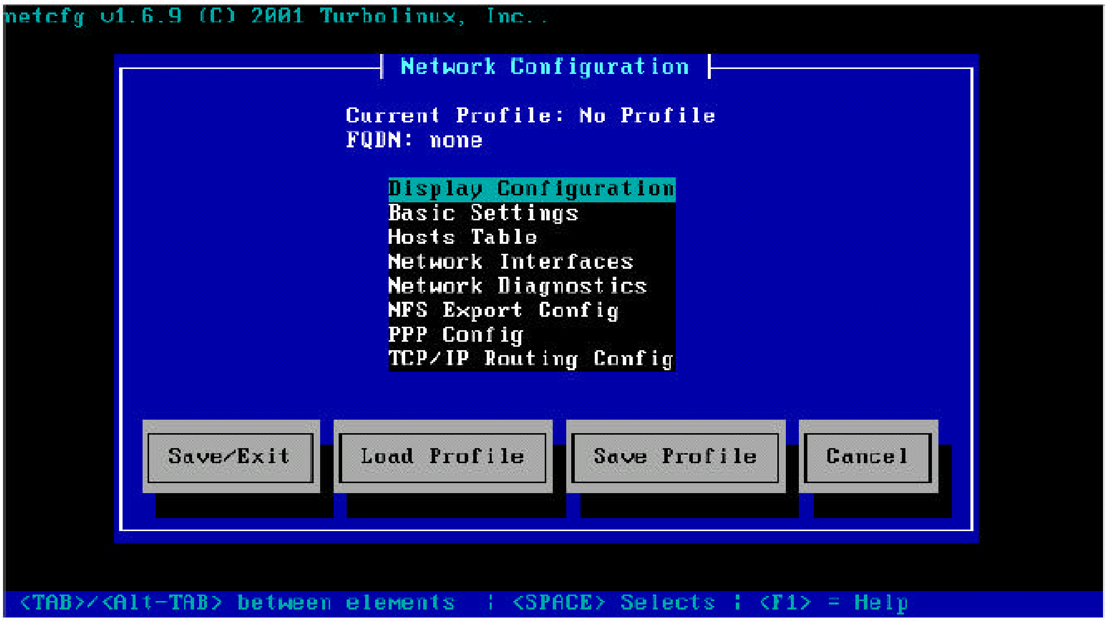
```
$ /sbin/ifconfig
```

使用工具网络进行配置

运行：

netcfg

这时，将出现“ Network Configuration **”（网络配置）屏幕**:



这些选项中的每一个均与网络有关：

- Display Configuration **（显示配置）**
- Basic Settings **（基本设置）**
- Hosts Table **（主机表）**
- Network Interfaces **（网络接口）**
- Network Diagnostics **（网络诊断）**

亮选希望配置的条目，并按下回车键。

你可以使用 netcfg **来设置轮廓文件，以便能够方便地在多种配置间进行切换。一旦建立了一个新的轮廓文件，可按下“** Save Profile **”（保存轮廓文件）按钮将它保存下来。应使用易于识别的名称来保存该文件。随后，要想切换到任何已有的轮廓文件，可选择‘** Load Profile **”（加载轮廓文件），然后选择所需的轮廓文件。**

注意：

在默认情况下，最初不会配置任何轮廓文件。当你未创建轮廓文件，同时却选择了“ Save Profile **”（保存轮廓文件）时，会出现消息“保存轮廓文件失败”。如果打算更改配置，首先应选择“** Save Profile **”（保存轮廓文件），然后创建一个新的轮廓文件。**

显示配置

在“网络配置”屏幕上选择“ Display Configuration **”（显示配置），请参见第** 2-33 **页上的图** 2-7**，这时将出现“当前配置”屏幕（请参见图** 2-8**）。**

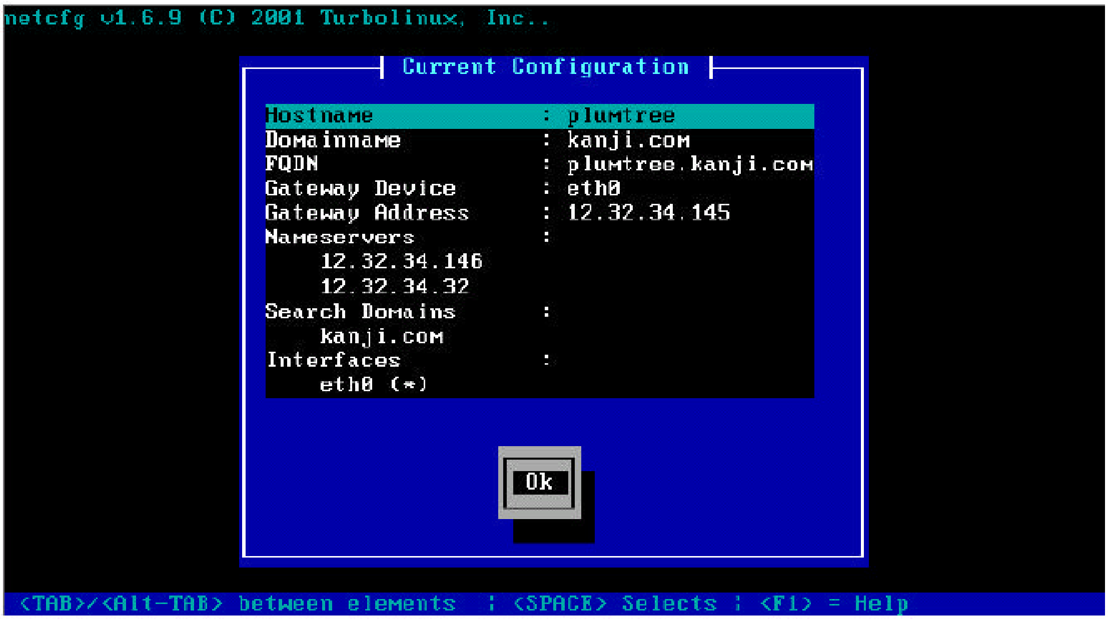


图 2-8 **当前配置**

在该屏幕上，显示了当前网络设置的状态。选择 “ OK **” (确认)按钮可关闭该屏幕。**

基本设置

在 “ 网络配置 ” 屏幕上选择 “ Basic Settings **” (基本设置)，请参见第** 2-33 **页上的图** 2-7**，这时将出现 “ 全程网络设置 ” 屏幕（请参见图** 2-9**）。**

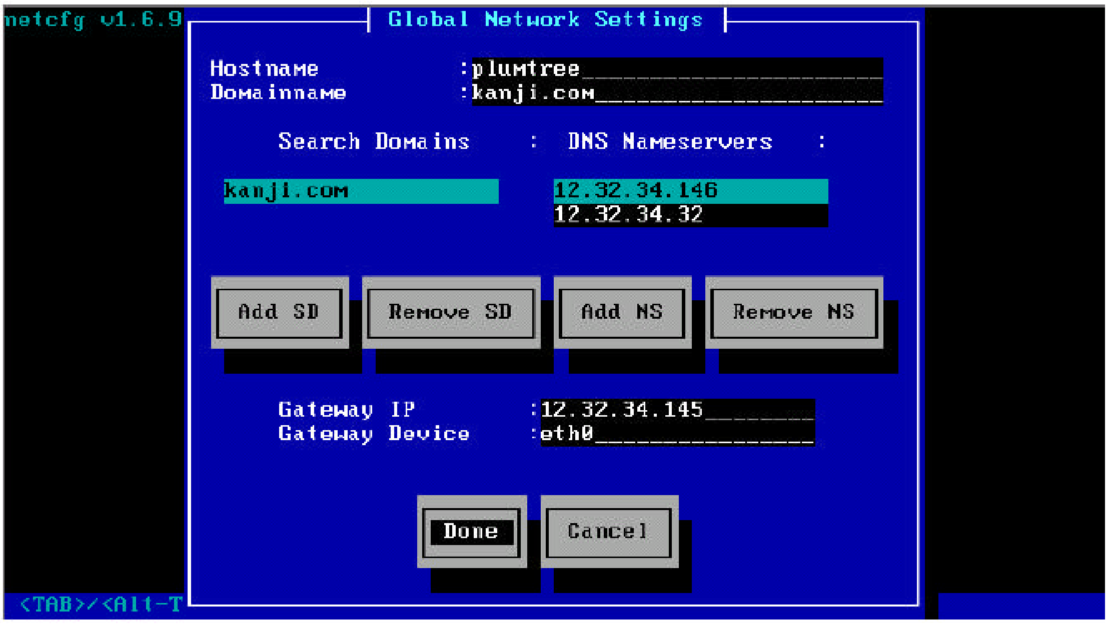


图 2-9 **全程网络设置**

在该屏幕上，你可以进行下述设置：

Hostname（主机名）	Turbolinux 计算机的主机名
Domainname（域名）	计算机所在网络的域名
Search Domains（搜索域）	进行搜索的域（通常与域名中给出的相同）。按下“ Add SD”可添加一个搜索域，使用“Remove SD”可删除搜索域
DNS Nameserver 域名服务器	DNS 服务器的 IP 地址。按下“ Add NS”可添加一个 DNS 域名服务器，使用“Remove SD”可删除 DNS 域名服务器。
Gateway IP（网关 IP）	默认网关的 IP 地址
Gateway Device（网关设备）	与上面的默认网关对应的网络接口卡。正常情况下，如果你只安装了一块网卡，它将被设置为“ eth0 ”。

主机表

在“ 网络配置 ”屏幕上选择“ Hosts Table ”（主机表），请参见第 2-33 页上的图 2-7，这时将出现“ 主机表 ”屏幕（请参见图 2-10）。

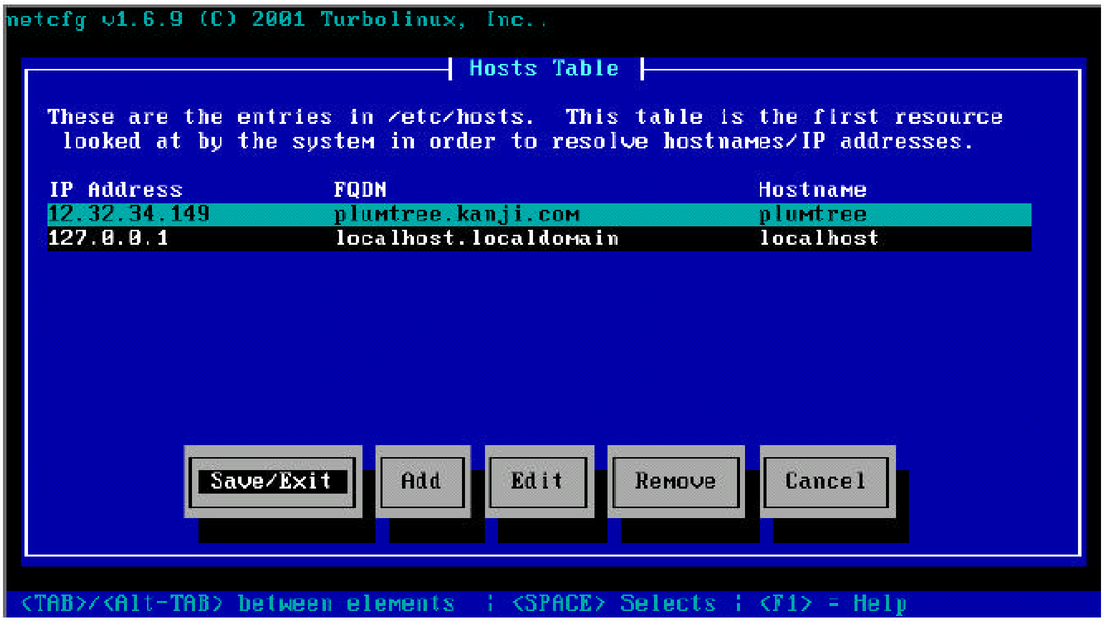


图 2-10 主机表

在该屏幕上，会显示来自文件/etc/hosts 的信息。通过该屏幕，你可以添加、更改、和删除主机。

网络接口

在“ 网络配置 ”屏幕上选择“ Network Interfaces ”（网络接口），请参见第 2-33 页上的图 2-7，这时将出现“ 选择接口 ”屏幕（请参见图 2-11）。

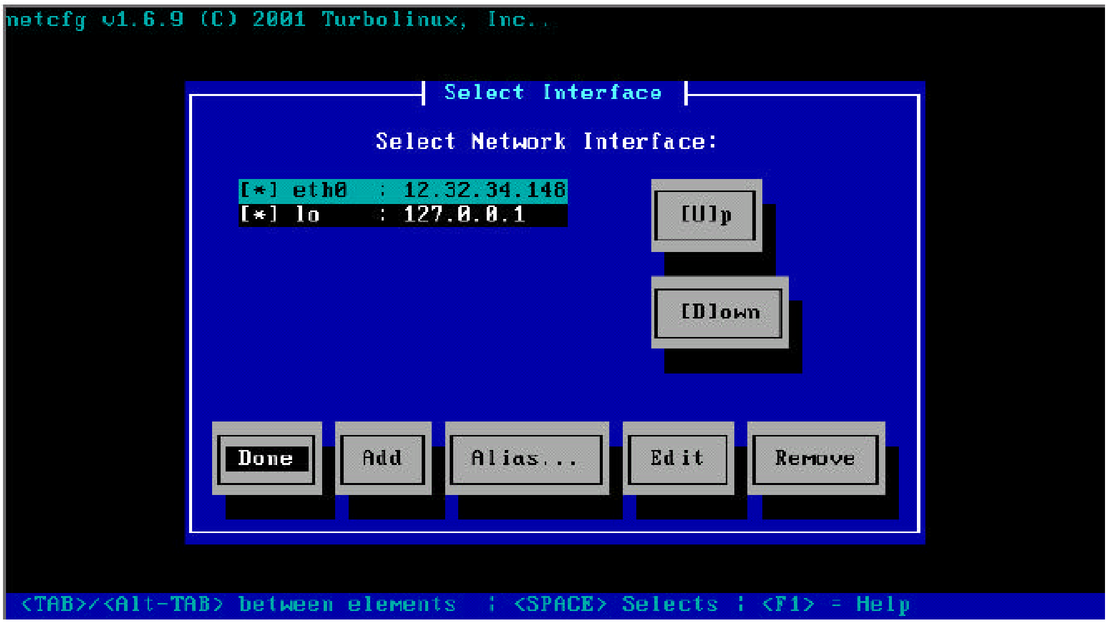


图 2-11 选择接口

在该屏幕上，你可以为每个网卡设置接口。

通常情况下，你只安装了一块网卡，这时你可以使用两个接口，“ lo ”（本地主机）以及“ eth0 ”。如果你安装了两个或更多的网卡，可以使用“ eth1 ”、“ eth2 ”等。

通过选择“ start ”（启动）和“ stop ”（停止），你可以在实时情况下启动或停止所选择的接口。

要想添加网卡，请选择“ Add ”（添加）；要想删除网卡，可选择“ Remove ”（删除）。

要想编辑所选择的接口，可在“ 选择接口 ”屏幕上选择“ Edit ”（编辑），请参见第 2-39 页上的图 2-11，这时，将出现“ 编辑接口设置 ”屏幕（请参见图 2-12）。

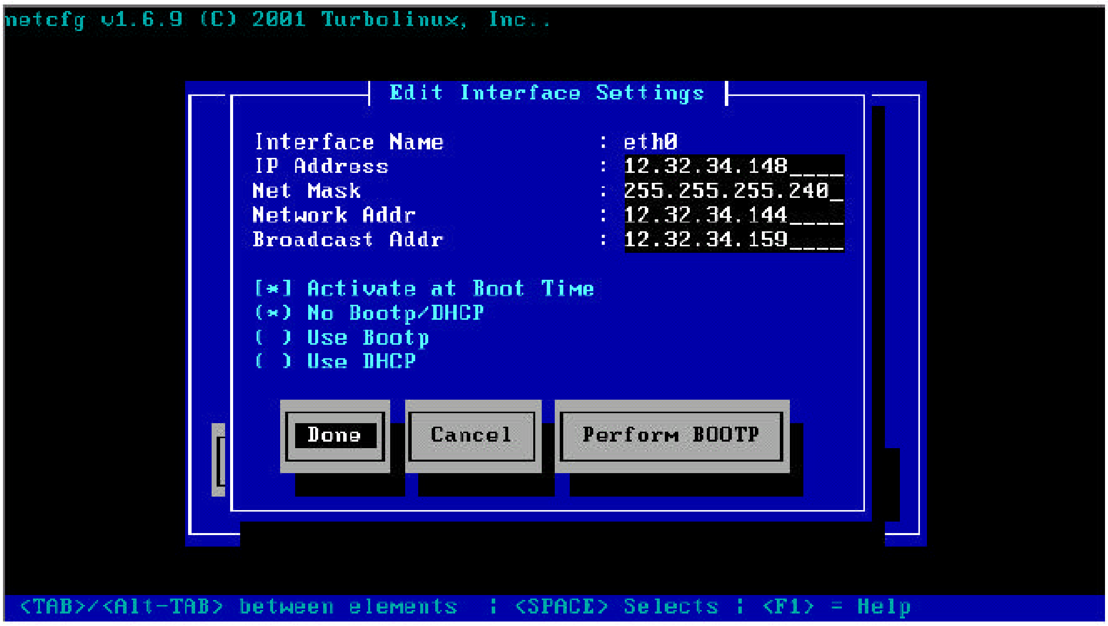


图 2-12 编辑接口设置

在该屏幕上，你可以设置下述条目：

• IP address （IP 地址）
• netmask （网络掩码）
• network address （网络地址）
• broadcast address （广播地址）
• Use of DHCP/Bootp （使用 DHCP/Bootp）

选择 “ Done ” （完成）可将你做的新设置保存下来，使用 “ <ESC> ” 键可放弃对当前设置的更改并返回 “ 选择接口 ” 屏幕（请参见图 2-11）。

• 在 “ aliases ” （别名）下，可为一个接口设置多个 IP 地址。

然后，使用 “ Done ” （完成）按钮，返回 “ 网络配置 ” 屏幕上的主菜单（请参见第 2-33 页上的图 2-7），并选择 “ 网络诊断 ” 以测试默认的路由路径、域名服务器的可达性等。这是会出现 “ 测试结果 ” 屏幕（请参见图 2-13）。

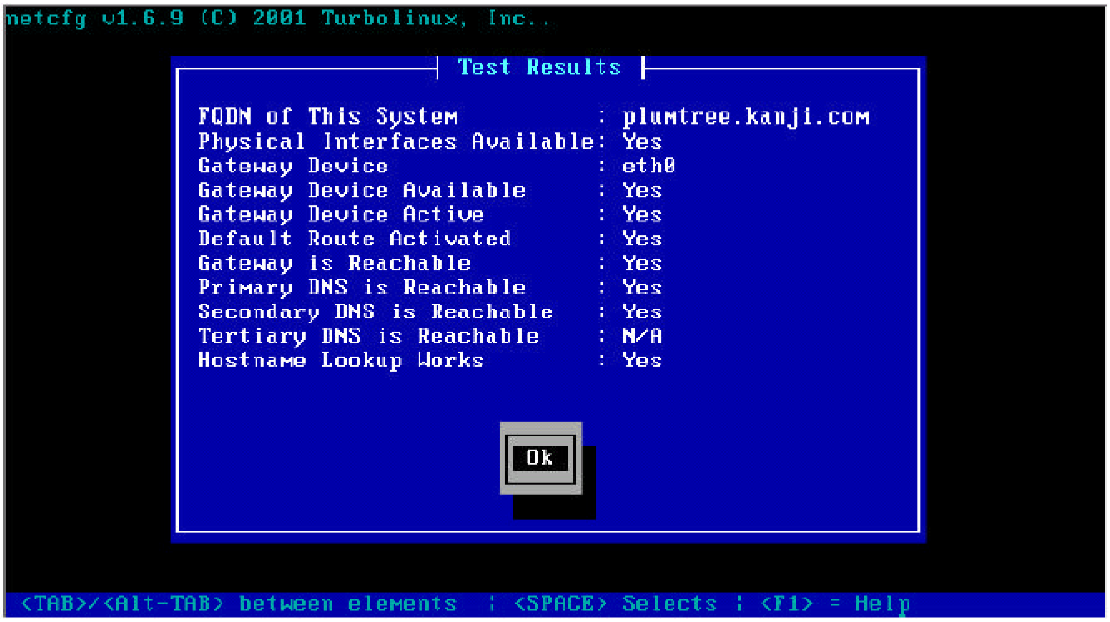


图 2-13 测试结果

在这个“测试结果”屏幕上（请参见第 2-41 页上的图 2-13），给出了每个条目的结果。“Yes”表示功能运行正常，“No”意味着出现了某些问题，“N/A”表示该条目尚未设置。选择“OK”，可显示“接口统计”屏幕（请参见图 2-14）。

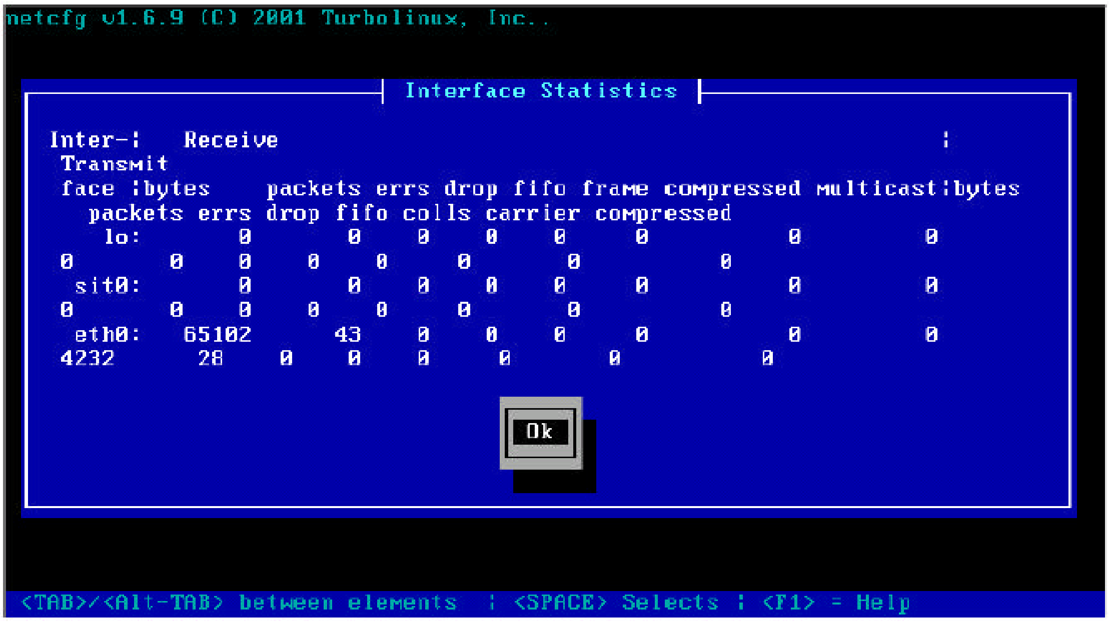


图 2-14 接口统计

4.6 打印

使用 Turbolinux 的工具 printconfig（turboprintcfg）可对你的服务器进行设置，以便打印文档和文件。在本节中，介绍了在 Turbolinux 环境下对打印进行组织的方法。

对于 Linux 下的打印来说，无论输出的是文本还是图形，都是通过 PostScript 输出来完成的。如果你有一台支持 PostScript 的打印机，就可以将输出直接发送给它。

要想进行非 PostScript 打印，就需要专门的 Linux 驱动程序。请与你的打印机制造商联系，了解这方面的情况。

4.6.1 Ghostscript

通过它的 PostScript 解释器，Ghostscript 能将转换后的 PostScript 数据按某种格式输出，该格式可很多打印机接受。通过使用 Ghostscript 解释器，可以将数据输出给很多常见的非 PostScript 打印机。

首先，请检查你的打印机是否与 Ghostscript 兼容。可以参考命令 gs –h 的输出，参考 /usr/share/doc/packages/ghostscript-6.51/目录下的文档。

/etc/printcap

可以在文件/etc/printcap 中编辑与打印机设备有关的设置。

下面给出了对连接到并口的 PostScript 打印机的设置：

(1)|lp:\
(2)|:sd=/var/spool/lpd/lp:\
(3)|:mx#0:\
(4)|:sh:\
(5)|:lp=/dev/lp0:\
(6)|:if=/var/spool/lpd/lp/filter:

其中：

（1） 指出了打印机的名称，在本例中为“lp”。

（2） 指出了缓冲（也称为假脱机）目录，在本例中被设置为/var/spool/lpd/lp。

（3） 设置最大的文件容量，在本例中为“0”，表示对文件的大小不做限制。

（4） 禁止打印题头。要想打印题头，请删除该行。

（5） 设置打印机设备的名称，在上面所给出的示例中为“/dev/lp0”。

（6） 指定输入文件。由于在本例中使用的是 PostScript 打印机，所以输入文件为“/var/spool/lpd/lp/filter”。

完成编辑任务后，请重新启动 lpd。

/etc/rc.d/init.d/lpd restart

命令 lpr

使用命令 lpr，可进行打印操作。

例如，如果想在当前目录下打印文件 README.txt，可键入下述命令：

$ lpr README.txt

要想将发送给打印机的输出显示在屏幕上，而输出内容很长，无法在一个屏幕上显示出来，可对 lpr 使用管道命令。例如，如果打算将命令 ls 的输出结果发送给打印机，可运行：

$ ls | lpr

当你有多台打印机可供选择时，可使用-P 选项，后跟所选的打印机名称，这样可将文件发送给指定的打印机。

$ lpr -P lp0 README.txt

4.6.2 printconfig – turboprintcfg

使用工具 printconfig (turboprintcfg)，可添加和配置打印机。要想启动该工具，可键入命令：

printconfig

这时，会出现“配置打印机”屏幕（请参见图 2-15）。



图 2-15 **配置打印机**

添加打印机

要想添加并设置一台新的网络打印机，请按下述步骤进行：

1． **在“配置打印机”屏幕上选择“**Add**”（添加），请参见第** 2-45 **页上的图** 2-15。**出现“添加打印机”屏幕（请参见图** 2-16）。

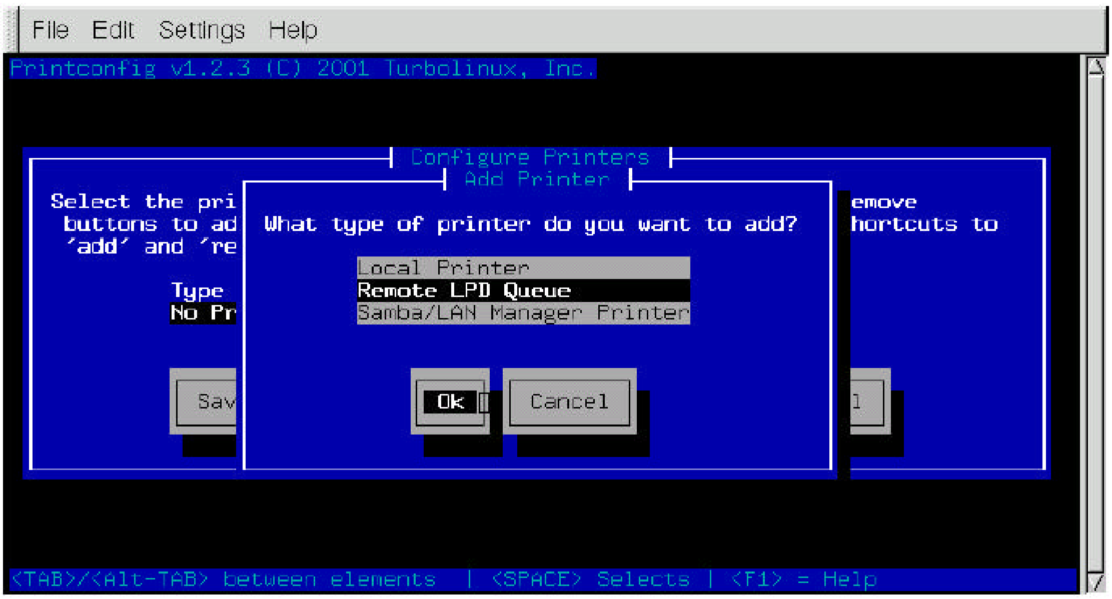


图 2-16 添加打印机

3． 为打印机选择连接类型。

Local Printer （本地打印机）	如果打印机直接连接在你的计算机上，请选择该选项。
Remote LPD Queue （远程 LPD 队列）	如果你打算使用 linux(unix)网络共享的打印机，请选择该选项。
Samba/LAN Printer （网络打印机）	如果你打算使用 windows 网络共享的打印机，请选择该选项。

对于本例，选择了“Remote LPD Queue”（远程 LPD 队列），并选择了“OK”。选择“OK”后，将出现“新队列名称”屏幕（请参见图 2-17）。

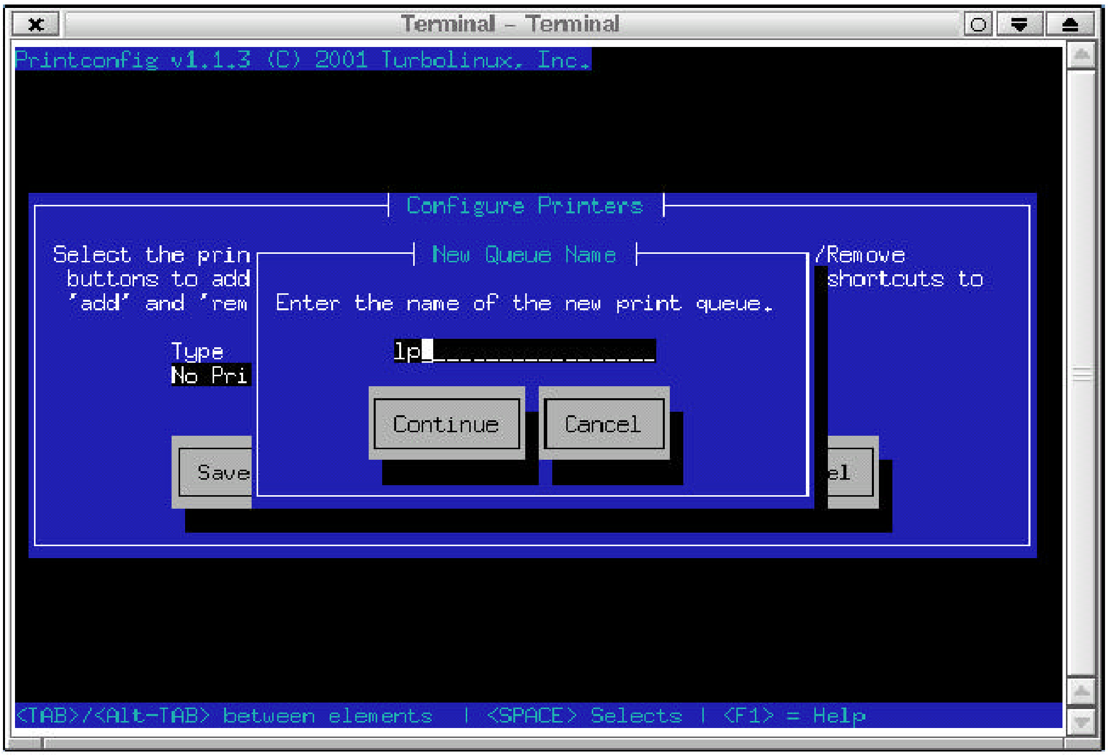


图 2-17 新队列名称

3. 设置执行打印作业时要使用的打印队列名称。正常情况下，使用默认设置“lp”。

4． 选择“Continue”(继续)。

5． 对于“LPD Settings”(LPD 设置）条目，亮选“Configure”(配置）字段，并按下回车键。这时将显示对应的字段：Remote Host Name（远程主机名称）以及 Remote Queue（远程队列），如图 2-18 所示。为这些字段输入值。

Remote hostname(远程主机名):远程共享出打印机的主机名;

Remote queue(远程队列名):通常是 lp 。

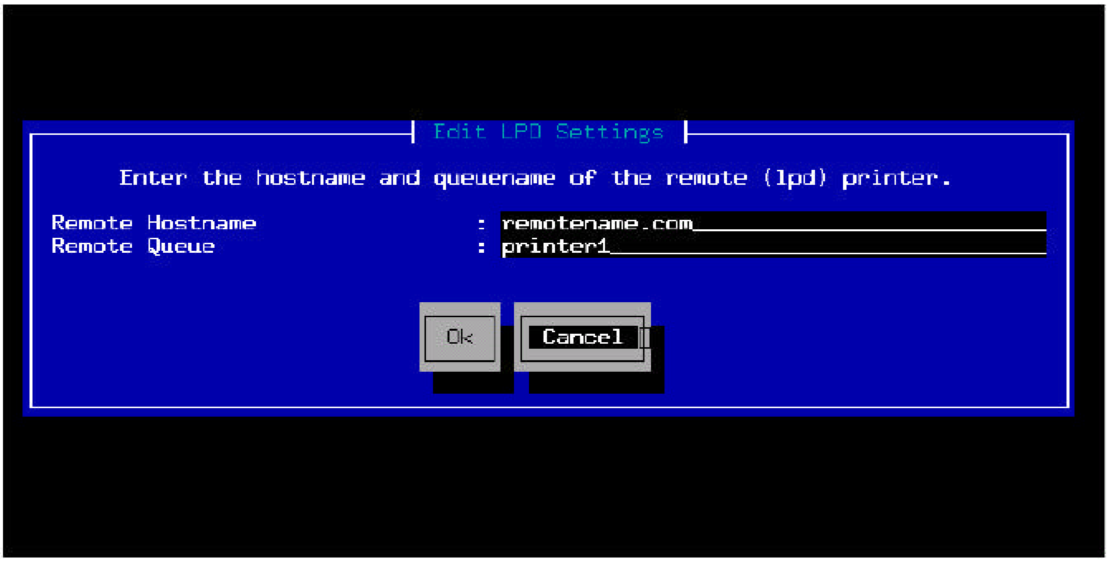


图 2-18 编辑 LPD 设置

6。 完成后，选择“OK”，然后选择“Save & Exit”(保存并退出)。

更改打印机设置

要想更改已有打印机的设置，请按下述步骤进行：

1。 在“配置打印机”屏幕上选择“编辑”(请参见第 2-45 页上的图 2-15)，出现“编辑打印机设置”屏幕（请参见图 2-19)。

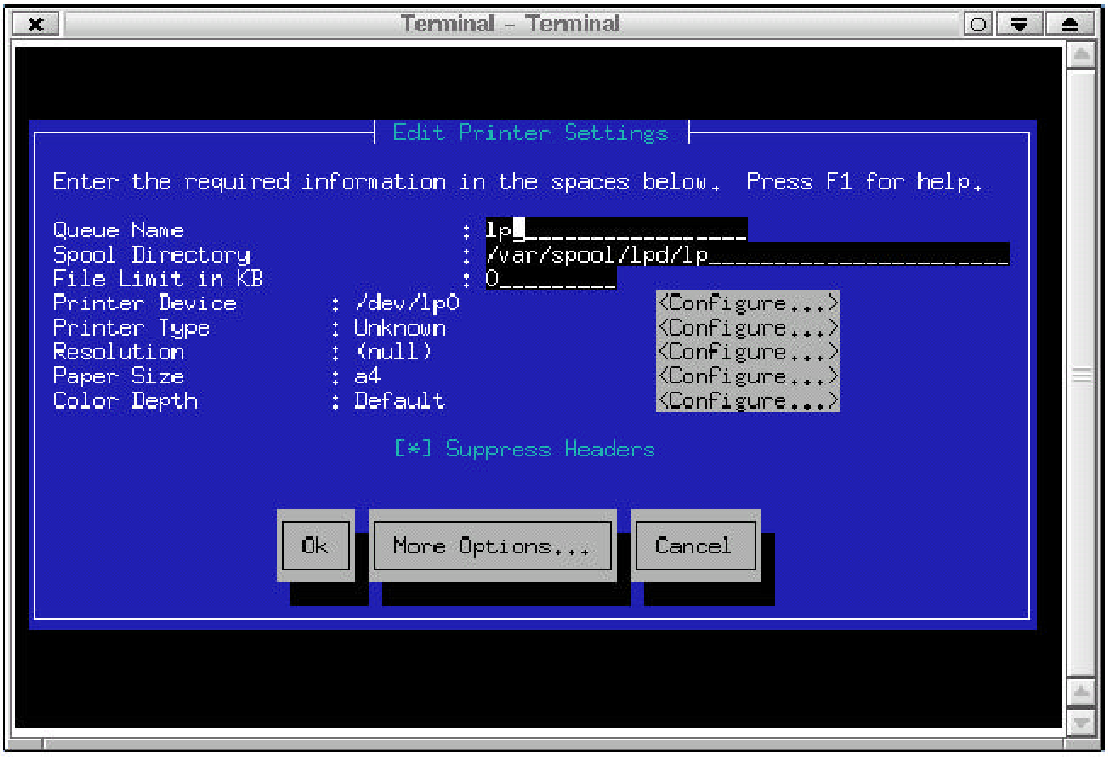


图 2-19 编辑打印机设置

2。 根据需要编辑设置。

3。 完成后，选择“OK”(确认)返回主“printconfig”屏幕。

第五章　Internet 服务器

网络世界中处于运行状态的服务器总会做好随时应答来自客户端请求的准备。另一方面，仅在需要发送请求时，才会运行客户端相应程序。在用户层面，客户端－服务器操作是透明的，也就是说，不需要用户的了解任何细节过程以及任何介入。

此外，还存在多种超级服务器，这些超级服务器负责控制普通服务器。只有当收到来自客户端的请求时，超级服务器才会触发普通服务器上提供相应服务。

在本章中，详细介绍与所列的四种服务器有关的信息。这些服务器能提供四种基本的服务，Turbolinux 提供的这四种服务，可以另您的网络更好的发挥作用。

• 域名服务器（DNS 服务器）：查找主机名称的 IP 地址。

• 邮件服务器（SMTP）：在网络的主机之间传递电子邮件。

• Web 服务器（HTTP 服务器）：使用了 HTTP 协议完成客户端程序（浏览器）对 Web 页面、文件、来自 Internet 的数据、或来自本地系统或网络的数据的请求。

• FTP 服务器：接收来自其它主机的文件或向其它主机发送数据。

5.1　域名服务器（DNS 服务器）

域名服务器（域名系统服务器、或 DNS 服务器）的作用就是从主机名称查找对应的 IP 地址，或者相反，IP 地址查找其主机名称。实现该任务的一种方法是使用文件/etc/hosts。在这种情况下，每台主机本身会查找自己的/etc/hosts 文件。如果使用 DNS 服务，在相同的域中必须至少有一台 DNS 服务器，以便主机的名称信息提供给该域范围的其它多台主机。

为了实现 DNS 功能，最常用的程序是 BIND。要想了解有关 BIND 的详细信息，请参后面的“BIND 概述”。

可以将域名服务器的作用划分为下述四类：

• Primary Name Server（主域名服务器）

• Secondary Name Server（从域名服务器）

• Cache Only Server（高速缓冲服务器）

• Slave Server（从属服务器）

5.1.1　主域名服务器

主服务器负责管理自己所在域内的所有主机名称，确保向本域的其它服务器提供信息，并负责与其它域的域名服务器交换信息。

5.1.2 从域名服务器

从域名服务器以主域名服务器的备份形式存在。它会定期拷贝来自主域名服务器的数据，如果主域名服务器出现故障，它将接替主域名服务器。这两个服务器（主服务器和从服务器）中必须至少有一个能正常地发挥作用，从而保证与 Internet 的正常连接。

5.1.3 高速缓冲服务器

高速缓冲服务器能将客户端的请求转发给它所指定的域名服务器。正如其名称所表示的那样，高速缓冲服务器只会临时性（以缓冲方式）地保存应答信息，这样当它下一次收到相同的请求时能更快地作出响应。这样，就能减轻主域名服务器和从域名服务器的负担。

5.1.4 从属服务器

从属服务器负责维护与主域名服务器相同的数据库，但在它解析请求之前，必须得到主服务器的许可。

5.1.5 解析器

解析器负责将来自客户端的请求转发给域名服务器，然后将来自服务器的回答信息返回给客户端。域名服务器对解析器的查询作出响应，然后解析器对该信息（可能是资源记录或一则错误信息）进行解释，并将结果递送给启动请求的程序。

在解析服务器和客户端名称时，需要用到下面这两个文件：

/etc/host.conf
/etc/resolv.conf

文件/etc/host.conf 是为名称服务请求而创建的，它创自于域名服务器以及传统的 UNIX 主机文件。

每台主机必须列在主机文件中，对于大型网络来说，这会使得主机文件变得笨拙和不切实际。但对于由四个或五个主机构成的小型网络来说，域名服务器所承担的负荷较轻，它能很好地胜任。

下面是文件/etc/host.conf 的一个示例：

```
order hosts,bind
multi on
```

在上面的示例中，order 显示出了执行的顺序。这意味着首先将使用主机文件来解析名称，如果失败，再使用 BIND。

如果名称解析导致了多个地址，那么 multi on 表示会返回所有的地址，multi off 表示只返回第 1 个地址。

在文件/etc/resolv.conf 中，包含域名和域名服务器方面的信息。

下面给出了文件/etc/resolv.conf 的一个示例：

```
domain turbolinux.gr.cn
search turbolinux.gr.cn
nameserver 192.168.0.2
```

在上面的示例中，domain 指的是服务器的域名，search 指的是用于主机查询的搜索域名，nameserver 指的是解析器应查询的域名服务器地址。

5.1.6 BIND 概述

BIND 诞生于加利福尼亚大学伯克利分校，首先出现于 BSD UNIX 4.3 版本中。自那以来，它已被引入到 Linux、其它 UNIX 版本、OS/2、以及 Windows NT 中。

直到推出 4.8.3 版本前，对 BIND 的开发一直是在 DAPRA 的同意下，在加州大学伯克利分校的计算机系统研究小组中进行的。版本 4.9 和 4.9.1 由当时的 DEC（即现在的康柏）发布。其 4.9.2 版由 Vixie Enterprises 发布。自 4.9.3 版起，由 Internet 软件联盟（ISC）负责开发和维护。1997 年发布了版本 8，自那以后，除了偶尔发布的安全补丁外，对版本 4 的研发已终止。最近出现了版本 9（请参见下面所列出的 ISC 的 Web 站点）。

在下面的列表中，给出了一些缩略语的意义：

• BIND （伯克利 Internet 名字域），Web 站点：http://www.isc.org/bind.html

• DARPA（美国国防部高级计划研究局）

• UCB （加利福尼亚大学伯克利分校）

• CSRG （计算机系统研究组）

• ISC （Internet 软件联盟），Web 站点：http://www.isc.org/

有三种版本的 BIND 是以免费软件的形式发布的，分别是版本 4，版本 8 和版本 9。

某些 Internet 服务提供商推荐使用 BIND 4，这是因为它的稳定性和安全性，版本 4 已经得到了广泛的使用，作为一个良好的技术产品，它还拥有很高的声望。

然而，除了安全补丁外，对版本 4 的开发已终止，而且当前开发的源代码由 ISC 负责。因此，我们更推荐大家转换到版本 8 上。在本节中，我们将介绍对 BIND 4 的配置。在“ BIND 8 ”中，介绍了转换到 BIND 8 的方法。

named

BIND 主药由端口监控程序 named 构成。它的启动脚本是/etc/rc.d/init.d/named。

要想启动 named，可运行：

/etc/rc.d/init.d/named start

要想停止 named，可运行：

/etc/rc.d/init.d/named stop

如果想检查 named 正在运行，可：

ps aux | grep named

root 203 0.0 3.2 1440 1000 ? s 00:55 0:00 named

如果你未能见到与上面所给出的类似的响应，或许需安装 BIND。

域名服务器模式配置

BIND 能在三种模式下运行：

- Primary server mode（主服务器模式）
- Secondary server mode（从服务器模式）
- Cache Only server mode（高速缓冲服务器模式）

Turbolinux 7 Server 最初的默认设置是高速缓冲服务器模式。如果你的 ISP（Internet 服务提供商）同时经营着主服务器和从服务器，那么你所安装的域名服务器就可以作为高速缓冲服务器使用。要想实现这点，只需要两个配置文件：/etc/named.boot 和/etc/resolv.conf。现在以域名 turbolinux.gr.cn 为例，这些文件的内容如下。

文件/etc/named.boot：

```
directory /var/named
cache . named.ca
primary 0.0.127. in-addr.arpa named.local
```

文件/etc/resolv.conf：

```
domain turbolinux.gr.cn
search turbolinux.gr.cn
nameserver 127.0.0.1
```

对于主服务器和从服务器模式，这些设置会有所变化。

文件/etc/named.boot（请参见下面）用于从服务器模式，在本示例中，使用的 IP 地址是 192.168.0.2。

文件/etc/named.boot：

```
directory /etc/namedb
cache . named.root
secondary turbolinux.gr.cn 192.168.0.2 Turbolinux.zone.bak
secondary 0.168.192.in-addr.arpa 192.168.0.3 Turbolinux.rev.bak
secondary 0.0.127.in-addr.arpa local.rev
```

区域文件和逆向文件从主服务器、IP 地址 192.168.0.2 处获得，并会将它们备份到一个文件中。

5.1.7 典型设置

在这个示例中，使用的数据来自中国的 Turbolinux 域名服务器。当然，你也可以指定不同的主机名、IP 地址等。

在下面所列的 6 个设置文件中，除了/etc/named.boot 和/etc/resolv.conf 外，所有其他文件均任意。后者在文件/etc/named.boot 中指出。

文件名称	完整的文件名称
引导文件	/etc/named.boot
解析文件	/etc/resolv.conf
缓冲文件	/var/named/named.root
Lookback 文件	/var/named/0.0.127.inaddr.arpa
正向查找文件（区域文件）	/var/named/turbolinux.gr.cn
逆向查找文件	/var/named/2.0.168.192.in-addr.arpa

假设如下：

IP 地址	192.168.0.0~192.168.0.15
子网掩码	255.255.255.240
域名	turbolinux.gr.cn
从域名服务器	203.139.160.69 (hostname: ns-tk011.ocn.ad.jp)

如果你的 ISP（Internet 服务提供商）为你分配了 16 个 IP 地址，就可以按表 3-1 中给出的方式来组织你的域名服务器。

表 3-1 IP 地址与主机名称映射

IP 地址	主机名称	解释
192.168.0.0	无	网络地址（固定）
192.168.0.1	无	默认网关（路由器），通常是固定的
192.168.0.2	Ns.tubolinux.gr.jp	域名服务器（主），通常是固定的
192.168.0.3	Unixi.turbolinux.gr.cn	UNIX（或 Linux）终端
192.168.0.4	Wini.turbolinux.gr.cn	Windows 终端
192.168.0.5	Maci.turbolinux.gr.cn	Macintosh 终端
192.168.0.6	（可用）	
192.168.0.7	（可用）	
192.168.0.8	（可用）	
192.168.0.9	（可用）	
192.168.0.10	（可用）	
192.168.0.11	（可用）	

192.168.0.12	（可用）	
192.168.0.13	（可用）	
192.168.0.14	（可用）	
192.168.0.15	无	广播地址（固定）

注意：

不能使用表 3-1 **中所列的** IP **地址。你必须用你的** ISP **商分配给你的地址替换它们。**

5.1.8 引导文件（/etc/named.boot）设置示例

下面给出了一个示例用引导文件的内容：

(1) directory /var/named

(2) cache . named.root

(3) primary 0.0.127.in-addr.arpa 0.0.127.in-addr.arpa

(4) primary turbolinux.gr.cn turbolinux.gr.cn

(5) primary 2.0.162.192.in-addr.arpa 2.0.162.192.in-addr.arpa

下面，给出了对上述示例文件中条目的解释：

（1）**将** directory **设置为包含各配置文件的目录，在这里是**/var/named。

（2）**将** cache **设置为缓冲文件的名称。从**ftp://rs.internic.net/domain/named.root**处获取最新的文件。在这里，最新的文件被设置为** named.root。

第 1 **个主服务器用于回送，第** 2 **个用于正向查找文件（区域文件），第** 3 **个用于逆向查找文件。**

（3）**设置** lookback **文件的名称，在这里是** 0.0.127.in-addr.arpa

（4）**设置正向查找文件（区域文件），在这里是** tubolinux.gr.jp。

（5）**设置逆向查找文件，在这里是** 2.0.162.192.inaddr.arpa。

注意：

总应将网络地址的逆向处理写入到逆向查找文件

5.1.9 解析器文件（/etc/resolv.conf）设置示例

下面给出了一个示例用解析器文件的内容：

(1)| domain turbolinux.gr.cn

(2)| nameserver 192.168.0.2

(3)| nameserver 203.139.160.69

在上面的示例文件中，nameserver **被设置为域名服务器的** IP **地址。下面，给出了对上述示例文件中条目的解释：**

（1）domain **被设置为域名，在这里是** turbolinux.gr.cn。

（2）将主域名服务器（nemeserver）的 IP 地址设置为 192.168.0.2。

将从域名服务器（nemeserver）的 IP 地址设置为 203.139.160.69。通常情况下，该 IP 地址由 ISP 商指定。

至少，解析器文件必须包含主域名服务器和从域名服务器。

5.1.10 loopback 文件设置示例

在本节中，解释回送（loopback）文件/var/named/0.0.127.in-addr.arpa

0.0.127.in-addr.arpa. IN SOA ns.turbolinux.gr.cn.

root.ns.turbolinux.gr.cn. (

(1) | 19990318 ; Serial

| 10800 ; Refresh after 3 hours

| 3600 ; Refresh after 1 hours

| 604800 ; Expire after 1 week

| 86400) ; Minimum TTL of 1 day

(2) | 0.0.127.in-addr.arpa. IN NS ns.turbolinux.gr.cn

(3) | 0.0.127.in-addr.arpa. IN NS ns-tk011.ocn.ad.jp

| 1.0.0.127.in-addr.arpa. IN PTR localhost.

下面，给出了对上述示例文件条目的解释：

SOA	授权启动（Start of Authority）的缩写，用于设置区域管理信息。
IN	Internet 的缩写。
NS	域名服务器的缩写，用于设置域名服务器的主机名称。
PTR	打印机的缩写，为 IP 地址设置主机名称。
（1）	配置的序列号。任何初始值均是可接受的，但每次修改配置文件后，都必须增加它。这里使用了日期，便于记忆和日后的检查。
（2）	设置主域名服务器的主机名。在这里是 ns.turbolinux.gr.cn。
（3）	设置从域名服务器的主机名。通常情况下，它由你的 ISP 商指定，在这里是 ns-tk011.ocn.ad.jp。

5.1.11 正向查找文件（或区域文件）设置示例

区域文件/var/named/turbolinux.gr.cn 与下面所给出的相仿：

| turbolinux.gr.cn. IN SOA ns.turbolinux.gr.cn.

root.ns.turbolinux.gr.cn. (

(1) | 19990318 ; Serial

| 10800 ; Refresh after 3 hours

| 3600 ; Retry after 1 hours

| 604800 ; Expire after 1 week

| 86400 ; Minimum TTL of 1 day

(2) | turbolinux.gr.cn. IN NS ns.turbolinux.gr.cn.

(3) | turbolinux.gr.cn. IN NS ns-tkOll.ocn.ad.jp.

(4) | turbolinux.gr.cn. IN MX 10 ns.turbolinux.gr.cn.

(5) | localhost IN A 127.0.0.1

(6) | ns.turbolinux.gr.cn. IN A 192.168.0.2

(7) | unixi.turbolinux.gr.cn. IN A 192.168.0.3

(8) | wini.turbolinux.gr.cn. IN A 192.168.0.4

(9) | maci.turbolinux.gr.cn. IN A 192.168.0.5

(10) | mail.turbolinux.gr.cn. IN CNAME ns.turbolinux.gr.cn.

(11) | www.turbolinux.gr.cn. IN CNAME ns.turbolinux.gr.cn.

(12) | ftp.turbolinux.gr.cn. IN CNAME ns.turbolinux.gr.cn.

对上面示例文件中条目的解释如下：

MX	**邮件交换器的缩写**
A	**地址，为主机名设置** IP **地址**
CNAME	**规范名称的缩写，为主机设置别名**
（1）	**配置的序列号。任何初始值均是可接受的，但每次修改配置文件后，都必须增加它。这里使用了日期**
（2）…（3）…	**设置主服务器和从服务器的名称**
（4）	**设置邮件服务器的名称并显示优先级（优先级越高，数值越低）。在这里，主域名服务器和邮件服务器是相同的，因此优先级为** 10**，邮件服务器的主机名为** ns.turbolinux.gr.cn
（5）	**设置本地主机（**localhost**）的** IP **地址。**Localhost **表示其自身，在这种情况下，其** IP **地址通常是** 127.0.0.1**，如上所示**
（6）	**设置** ns.turbolinux.gr.cn **的** IP **地址**
（7）…（8）…（9）…	**为每台主机设置** IP **地址，在这里，它们是** unixi.turbolinux.gr.cn、wini.turbolinux.gr.cn、maci.turbolinux.gr.cn**，将它们的** IP **地址分别设置为** 192.168.0.3、192.168.0.4、**和** 192.168.0.5
（10）…（11）…（12）…	**设置别名（**CNAME**）。在这里，邮件服务器是** mail.turbolinux.gr.cn**，**Web **服务器是**www.turbolinux.gr.cn**，**FTP **服务器是**ftp.turbolinux.gr.cn。

5.1.12 逆向查找文件（或逆向文件）设置示例

逆向查找文件/var/named/2.0.168.192.in-addr.arpa **与下面所给出的相仿：**

| 2.0.168.192.in-addr.arpa. IN SOA

ns.turbolinux.gr.cn.

root.ns.turbolinux.gr.cn. (

(1) | 19990318 ; Serial

| 10800 ; Refresh after 3 hours

| 3600 ; Retry after 1 hours

| 604800 ; Expire after I week

| 86400 ; Minimum TTL of 1 day

(2) | IN NS ns.turbolinux.gr.cn.

(3) | IN NS ns-tkOll.ocn.ad.jp.

(4) | IN PTRturbolinux.gr.cn.

(5) | IN A 255.255.255.240

(6) | 2 IN PTR ns.turbolinux.gr.cn.

(7) | 3 IN PTR unixi.turbolinux.gr.cn.

(8) | 4 IN PTR wini.turbolinux.gr.cn.

(9) | 5 IN PTR maci.turbolinux.gr.cn.

(10)

对上面示例文件中条目的解释如下：

（1）	**对配置的序列号进行设置。任何初始值均是可接受的，但每次修改配置文件后，都必须增加它。这里使用了日期**
（2）… （3）…	**设置主服务器和从服务器的名称**
（4）	**执行针对域名所作的设置**
（5）	**设置子网掩码的地址，在这里是** 255.255.255.240
（6）…（7）…（8）…（9）…	**将** IP **地址的最后一个号码设置为相应的主机名**

在上面所讨论的示例文件中，即引导、解析、回送、正向查找、以及逆向查找文件中，你不能使用这里所给出的 IP **地址或主机名。你必须用自己的** ISP **商所指定的、位于你所在域中的恰当的** IP **地址替换它们。**

5.1.13 检查 BIND 配置

要想检查 BIND **是否运行正常，可使用命令** ping **和** nslookup**。**

首先，对自己执行 ping **命令，检查你自己的配置情况；然后，对你所在域中的其它主机执行** ping **命令；再接下来，对外部主机执行** ping **命令。下面，给出了对自身使用** ping **命令的示例，在本例中，自身的** IP **地址是** 192.168.0.2**（请用你自己的** IP **地址替换它）。按下组**

合键“ Ctrl+C ”可终止 ping 命令。此外，你还可以使用-cn 参数，仅显示 n 行数据。应使用正整数替换 n。

```
# ping -c5 192.168.0.2
PING 192.168.0.2 (192.168.0.2): 56 data bytes
64 bytes from 192.168.0.2: icmp-seq=O ttl=128 time=0.5 ms
64 bytes from 192.168.0.2: icrrp-seq=l ttl=128 time=0.5 ms
64 bytes from 192.168.0.2: icrrp-seq=2 ttl=128 time=0.5 ms
64 bytes from 192.168.0.2: icmp-seq=3 ttl=128 time=0.5 ms
64 bytes from 192.168.0.2: icmp-seq=3 ttl=128 time=0.5 ms
--- 192.168.0.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.5/0.5/0.5 MS
```

如果 ping 命令给出的结果与上面的类似，就表明你的本地网络工作正常。现在，可以试着对你所在网络内部和外部的主机执行 ping 命令。

可以按下述方式使用 nslookup 命令，检查 BIND 是否正在正常工作。

1． 首先，请确认在机器自己的 IP 地址和主机名之间的循环转换工作正常。

2． 同样，请确认在你所在域中，每台其它机器的主机名和 IP 地址之间的循环转换正常。

3． 最后，请确认外部主机（位于 Internet 上）的主机名和 IP 地址之间的转换正常。

4． 运行 nslookup（首次执行时，可能会延迟一段时间）。

```
# nslookup
Default Server: ns.turbolinux.gr.cn
Address: 192.168.0.2
Aliases: 2.0.168.192.in-addr.arpa
>
```

现在，请检查你是否能提取自己机器的名称和 IP 地址，是否能提取位于你所在网络内部和外部的其它主机的名称和 IP 地址。其结果应与下面所给出的类似：

> 后面表示您输入的命令,其下是结果显示.

```
> ns.turbolinux.gr.cn
ns.turbolinux.gr.cn
Address: 192.168.0.2

Name:     ns.turbolinux.gr.cn
Address: 192.168.0.2
> 192.168.0.2
Server: ns.turbolinux.gr.cn
Address: 192.168.0.2
```

```
Name: ns.turbolinux.gr.cn
Address: 192.168.0.2
```

你所在域中的其它主机…

```
> unixi.turbolinux.gr.cn
Server: ns.turbolinux.gr.cn
Address: 192.168.0.2

Name: unixi.turbolinux.gr.cn
Address: 192.168.0.3

> 192.168.0.3
Server: ns.turbolinux.gr.cn
Address: 192.168.0.2

Name: ns.turbolinux.gr.cn
Address: 192.168.0.2
```

外部主机…

```
> blue.ocn.ne.jp
Server: ns.turbolinux.gr.cn
Address: 192.168.0.2

Non-authoritative answer:
Name: blue.ocn.ne.jp
Address: 202.234.232.78

> 203.139.160.78
Server: ns.turbolinux.gr.cn
Address: 192.168.0.2
Name: blue.ocn.ne.jp
Address: 202.234.232.78
```

注意：
在上面给出的所有示例中，你必须用自己的主机名和相应的 IP 地址替换对应的内容。

5.1.14 BIND 8

默认情况下，Turbolinux **将安装** BIND 8**。使用文件** named.conf **可对** BIND 8 **进行配置，**

它的结构与 C 语言类似，是按照四种主要类别来组织的：

- named settings（named 设置）
- hint file settings（hint 文件设置）
- primary zone settings（主区域设置）
- secondary zone settings（从区域设置）

下面给出了用于文件 named.boot 和 named.conf 的脚本示例：

/etc/named.conf (BIND 版本 8)

```
options {
directory "/var/named";
/*
* If there is a firewall between you and nameservers
* you want to talk to, you might need to uncomment
* the query-source directive below. Previous
* versions of BIND always asked questions using
* port 53, but BIND 8.1 uses an unprivileged port
* by default.
*/
// query-source address * port 53 ;
};
zone "." {
type hint;
file "named.root";
};

zone "0.0.127.in-addr.arpa" {
type master
file "0.0.127.in-addr.arpa";
};

zone "turbolinux.gr.cn" {
type master;
file "turbolinux.gr.cn";
};

zone "2.0.162.192.in-addr.arpa" {
type master;
file "2.0.162.192.in-addr-arpa";
};
```

下面给出了对某些/etc/named.conf **设置的解释：**

options {...}	**为区域文件目录的配置文件设置默认值，等等。**
zone {...}	**在区域文件中定义区域**

当在区域语句中指定了“type hint**”时：它就会调用根域名服务器、或由** file **所指定的文件中的多个服务器。**hint zone **与** BIND 4 **中文件** named.boot **的缓冲相对应。**

当指定了“type master**”时：意味着由** file **所指定的文件将成为区域文件，而且** BIND **将作为该区域的主服务器启动。这与** named.boot **的主服务器相对应。**

当指定“type slave**”时，将生成主区域的一个副本。该设置是针对从服务器的。**

当指定“type stub**”时，仅生成** NS PR **的一个副本。**

同样在 BIND 8 **中，可以针对各区域设置查询限制、区域传递等。**

在下面，给出了针对专有区域、用于定义逆向查询文件的一个脚本示例。

```
zone "2.0.168.192.in-addr.arpa" {
type master;
file "rev/.192.168.0.2";
masters {
192.168.0.2;
};

allow-query {
192.168.0.2/24;
xxx.xxx.xxx.xxx/yy
127.0.0.1;
};

allow-transfer {
192.168.0.2/24
xxx.xxx.xxx.xxx/yy
};
}
```

允许的公共网络地址被记作 xxx.xxx.xxx.xxx/yy**。这样设置后，来自与** xxx.xxx.xxx.xxx/yy **不同的地址的所有查询和传输请求均将被拒绝。**

我们建议，你应指定 allow-query**（允许查询）和** allow-transfer**（允许传输），用它来限制域名服务器查询和区域传输请求，从而减少不必要的系统负载,使得潜在的安全漏洞尽可能小。**

5.2 邮件服务器

Turbolinux 7 Server 采用了 Sendmail 作为邮件传输代理（MTA，也称为报文传输代理），这是最流行的邮件服务器。关于这个使用最广泛的程序，相应的文档和参考资料十分丰富。不过，由于功能的强大,对 Sendmail 的配置还是有一定的难度的。

5.2.1 Sendmail

邮件服务器 Sendmail 为多种 MTA 设置了标准。设计 Sendmail 的目的是为了支持不同于 SMTP 的邮件传输过程.

但由于 SMTP 的普及和重要，我们将重点还是放在了解释 SMTP 的配置方面。

由于 Turbolinux 7 Server 采用了 procmail 来处理本地消息，故在这里不讨论 mail.local 功能。

仅安装 sendmail，并不能让 Sendmail 正常工作。你必须通过定制 sendmail.cf，创建一个适合于自己网络的邮件服务器。关于 Sendmail 的最新信息，请访问它的 Web 站点 http://www.Sendmail.org。关于安装和配置方面的帮助信息，请参阅 Turbolinux 发行版本所带的文档。在 Turbolinux 7 Server 中，该文档位于/usr/share/doc/packages/sendmail-doc-8.11.4 下的子目录内。在那里，你还能找到该文档的 PostScript 版本，可以直接将其打印出来。该文档被称为"Sendmail Installation and Operation Guide"（Sendmail 安装和操作手册），它是由 Sendmail 有限公司的 Eric Allman 编撰的。在站点http://www.sendmail.org/~ca/email/ 上还提供了该手册的在线版本，请参阅"Sendmail 文档"一节。

生成配置文件

建议你对文件 sendmail.cf 进行备份。然后根据网络设置该文件，同时除了系统管理员外，其他用户不能编辑该文件。

```
# mv /etc/sendmail.cf    /etc/sendmail.cf.old
# cp sendmail.cf    /etc/sendmail.cf
# chmod 644    /etc/sendmail.cf
# vi /etc/sendmail.cf
```

命令 sendmail

Sendmail 的运行时参数选项是：

选项	使用	关联命令
-bd	作为端口监控程序运行（端口 25）	smtpd
-bp	显示未发送的邮件队列	mailq
-bi	启用别名数据库	newaliases
-bt	在测试模式下运行	
-bv	验证地址（不搜集或传递邮件）	

测试操作

实际运行 Sendmail 前，必须测试它。关于测试模式下与 sendmail 有关的信息，请参阅在线 的 man page，以及“ Sendmail 安装和操作手册 ”中的合适章节。正如下面所阐述的那样，你还能够显示出在 cf 文件中定义的地址、查看它的实际操作、并发送邮件。

• cf 地址定义的内容如下（使用 ns.test.com.cn 作为例子）：

```
# sendmail -bt -d0 < /dev/null
Version 8.11.6
 Compiled with: MAP_REGEX LOG MATCHGECOS MIME7TO8 MIME8TO7 NAMED_BIND
                NETINET NETINET6 NETUNIX NEWDB NIS QUEUE SASL SCANF SMTP USERDB
                   XDEBUG
============ SYSTEM IDENTITY (after readcf) ============
      (short domain name) $w = sun
  (canonical domain name) $j = sun.dev.cn.tlan
         (subdomain name) $m = dev.cn.tlan
              (node name) $k = sun.dev.cn.tlan
========================================================
ADDRESS TEST MODE (ruleset 3 NOT automatically invoked)
Enter <ruleset> <address>
```

• 通过检验模式检查递送过程

当邮件发送不能正常工作时，通过该操作，你就能发现错误所在。在下面的示例中，user1 指的是本地用户。如果该用户不存在可以用命令 usradd user1 增加该用户.

```
# sendmail -v user1 </dev/null
user1 ... Connecting to pmlocal ...
user1 ... Sent
```

上面的系统应答证实：已执行了一项本地递送。

如果系统没有应答证明系统的 sendmail 可能没有运行可以这样启动 sendmail,然后再执行上述命令:

#/etc/rc.d/init.d/sendmail start

接下来，你可以尝试将邮件从另一台机器（例如，root@host1.turbolinux.gr.cn**）发送到** user1@test.com.cn**。假定** Sendmail **已经在** test.com.cn **的** MX **主机上运行。**

```
# sendmail -v user1@test.com.cn < /dev/null
user1@test.com.cn...Connecting to ns.test.com.cn.via esmtp...
220 ns.test.com.cn ESMTP Sendmail 8.9.3/3.7Wp12; Tue,
17 Aug 1999 20:56:16 +0900
>>> EHLO host1.turbolinux.gr.cn
250-ns.test.com.cn Hello IDENT:root@[192.168.2.80], please to meet you
250-EXPN
250-Verb
250-8BITMIME
250-SIZE
250-DSN
250-ONEX
250-ETRN
250-XUSR
250-HELP
>>>MAIL From:<root@host1.turbolinux.gr.cn>
250 <root@host1.turbolinux.gr.cn>... Sender ok
>>> RCPT To:<user1@test.com.jp>...Recipient ok
>>> DATA
354 Enter mail, end with "." on a line by itself
>>> .
250 UAA00530 Message accepted for delivery
user1@test.com.cn... Sent (UAA00530 Message accepted for delivery)
>>> QUIT
221 ns.test.com.cn closing connection
```

通过这种方式，就能理解邮件发送的状态。这表明邮件发送能被恰当地执行。

启动 Sendmail 端口监控程序

Sendmail **的启动脚本是**/etc/rc.d/init.d/sendmail。
主要的启动脚本选项为" start **"（启动）、"** stop **"（停止）和"** restart **"（重新启动）。**
如果你更改了 Sendmail **的配置，就必须重新启动它，这样才能是所做的更改生效。**
要想启动 Sendmail**，可运行：**

```
# /etc/rc.d/init.d/sendmail start
```

你可以启动 Sendmail 端口监控程序，并设置每小时要发送的队列。要想直接设置它们，可执行：

```
# sendmail -bd -q1h
```

要想停止 Sendmail，可：

```
# /etc/rc.d/init.d/sendmail stop
```

要想重新启动 Sendmail，可：

```
# /etc/rc.d/init.d/sendmail restart
```

如果想检查 Sendmail 的当前状态，可运行：

```
# ps aux | grep sendmail
root 351 0.0 3.7 1916 1164 ? S 08:13 0:00 sendmail : accepti
```

如果你未见到上面的响应，就表示 Sendmail 或是未运行，或是未安装 Sendmail。在这种情况下，你将不得不重新启动 Sendmail（就像上面所介绍的那样），或者重新安装 Sendmail。

5.2.2 POP/IMAP

要接收邮件，必须使用 POP 或 IMAP 等服务。下面给出了对 POP 和 IMAP 的一般性介绍。

启动 POP 服务器

POP 服务器是通过超级服务器端口监控程序来运行的。由于其定义已在 xinetd 配置文件目录中给出，你可以简单地将/etc/xinetd.d/pop-3 中"disable"的取值更改为"NO"。然后，运行下面给出的两个命令中的一个，重新启动 xinetd：

```
# killall -HUP xinetd
# /etc/rc.d/init.d/xinetd restart
```

这将运行 POP 服务器。

但是，由于访问控制，客户端必须具有恰当的权限才能访问 POP 服务器。

在文件/etc/hosts.allow 中添加如下内容增加该客户的访问权限,该内容或是本地地址、或是许可的其它 IP 地址，如 192.168.2.0 等。

```
ipop3d : 192.168.2
```

如果允许该主机使用包括 pop 的所有的服务，添加下行内容：

```
ALL : 192.168.2.
```

关于更多的信息，请参见后面的"xinetd"或上面的"访问控制"。

启动 IMAP 服务器

IMAP 服务器也是通过超级服务器端口监控程序来运行的，你只需要将文件/etc/xinetd.d/imap 中的“disable”值更改为“NO”即可。

文件 hosts.allow 中的设置同上。然后重新启动 xinetd。

5.2.3 邮件管理

邮件管理包含下述任务：

- 建立邮件缓冲区，为单独用户保存未阅读的邮件。
- 设置邮件转发功能。
- 管理邮件队列。

邮件缓冲区

当邮件服务器收到邮件并将邮件发送给本地用户时，邮件将保存在该用户的文件/var/spool/mail 中。该文件包含用户尚未阅读的消息。每次分发新邮件时，都会将新邮件附在该文件上。

在下面的示例中，给出了针对用户 foo 和 student1 的邮件缓冲区：

```
# ls -l /var/spool/mail
-rw-rw---- 1 foo root 329 Aug 18 17:08 foo
-rw-rw---- 1 student1 root 5156 Aug 01 08:00 student1
-rw------- 1 rppt rppt 6812 Aug 18 18:23 root
```

当用户提走他的邮件时，邮件缓冲区将被清空。如果在用户读取邮件的过程中出现中断，那么该邮件将以 mbox 格式保存在用户主目录下的文件中。

邮件别名功能，可以将一个接收地址转换为一个或多个易于理解的其他接收地址。一般而言，别名功能用于为邮件服务器上的本地用户指定替代的名称，或将定址为列表将一个邮件分发给多个用户。

别名功能的标准文件是/etc/mail/aliases。该文件的格式是“local account: alias”（本地账户：别名）。因此，要想为本地账户“user1”指定别名“foo”，可以：

```
user1: foo
```

这样，user1 也能接收针对 foo 的邮件。

此外，使用下面的设置，也能将一般情况下针对超级用户(root)的错误信息发送给 foo 和 student1。

```
root:foo,student1
```

更改了任何别名设置后，要想确保在别名数据库中反映出这些变动，应使用下述命令执行更新操作：

newaliases

邮件转发

使用该项功能，可将目标为你自己的邮件转发给不同的地址。

文件.forward **被放在单独用户的主目录下。例如，如果向将目标地址为** foo@test.com.cn **的所有邮件转发给** student1@usa.edu**，可以用所需的目标地址创建文件**/home/foo/.foward**：**
student1@usa.edu

现在，目标地址为 foo@test.com.cn **的邮件不会被发送到** foo **的邮箱中，而是会被发送到** student1@usa.edu**。**

管理邮件队列

出于某种原因，不能正确发送邮件时，会将该邮件临时保存在目录/var/spool/mqueue **下，以后再发送。**

要想查看邮件队列中的内容，可运行：

```
# mailq
```

每隔一定的时间间隔，就会再次发送位于该队列中的邮件。如果采用了启动脚本来运行它，大约每隔一个小时会再次发送（带选项-qlh**）。如果打算强制执行重新发送，可运行：**

```
# sendmail -q –v
```

位于" queue **"（队列）目录下的邮件会被分成数个部分，并被保存在多个单独的文件中。文件类别是：**

文件标识符	解释
Df	消息主体
Qf	队列控制文件（和题头）
Xf	副本文件
Tf	用于 qf 重写的临时文件

按下述方式运行命令 ls**，可查看邮件队列：**

```
# ls /var/spool/mqueue
dfPAA01994 qfPAA01994
```

上述响应表明，对于队列 ID PAA01994 **来说，存在一个邮件队列控制文件（**qf**）和一个消息主体文件（**df**）。**

如果出于某种原因，删除了队列中的邮件，应立刻删除该目录下的这些文件。执行该类操作时，不要将邮件的 ID **弄混。**

```
# cd /var/spool/mqueue
# rm *PAA01994
```

通过伪造队列内容等方式,可以很容易地开启安全漏洞,正因为如此,只有超级用户(root)才有权读取和更改 mqueue 目录。你可以按下述方式设置该许可：

```
# chmod 700 /var/spool/mqueue
```

5.3 Web 服务器

Web 服务器也称为 WWW 服务器或 HTTP 服务器，支持 WWW 上的超文本传输协议。采用 HTTP 协议下载客户端（例如，浏览器）所请求文档、任何相关的 HTML 文件、图形和脚本。

HTTP 是一种网络上用于交换由 HTML 所写的 Web 文件的协议，WEB 服务器能够为使用 HTTP 协议的 Web 页面提供服务，它是公共 Web 站点服务器端的独立的程序。通过下面所列的 Web 站点，可以了解到有关 WWW、HTTP 和 HTML 方面的信息：

- WWW (环球网) http://www.w3.org/WWW/
- HTTP (超文本传输协议) http://www.w3.org/Protocols/
- HTML (超文本链接标示语言) http://www.w3.org/MarkUp/

世界上的第 1 个 Web 服务器是在 1991 年 6 月,以 CERN(欧洲粒子物理研究所)的 httpd 和 NCSA（美国国家超级计算应用中心）的 HTTPd 形式发布的。现在，对这两种版本的开发均已停止（CERN 的 httpd 于 1996 年四月停止开发）。自那以来，不断开发出了各种基 Web 服务器，如基于 java 的 Jigsaw，以及世界上最流行的 Web 服务器 Apache（阿帕奇）。下面给出了数个与这些服务器有关的 Web 站点：

- CERN（欧洲粒子物理研究所），http://www.cern.ch/
- CERN httpd，http://www.w3.org/Daemon/
- NCSA（（美国国家超级计算应用中心）），http://www.ncsa.edu/
- NCSA HTTPd，http://hoohoo.ncsa.uiuc.edu/
- W3C（WWW 联盟），http://www.w3.org/
- Jigsaw，http://www.w3.org/Jigsaw/
- Apache，http://www.apache.org/

5.3.1 Apache（阿帕奇）概述

Apache 是世界上使用最广泛的 Web 服务器。根据最新的统计数据，世界上 60%以上的 Web 服务器运行的都是 Apache。它已成为事实上的标准。它由 Apache 项目组负责开发。Apache 是一种免费、稳定、快速和易于管理的 Web 服务器。它具有丰富、良好的特性，而

且它的源代码是向公众公开的。

从开发者“ Apache 项目组 ”的 Web 站点上，可以获得有关 Apache 方面的信息。Ezine ApacheWeek 也提供了有关 Apache 的信息。

- The Netcraft Web Server Survey，http://www.netcraft.com/survey/
- Apache Project，http://www.apache.org/
- About Apache Project，http://www.apache.org/ABOUT_APACHE.html
- ApacheWeek，http://www.apacheweek.com/

在 Internet 上，通过 Apache 项目的 Web 站点和多种镜像站点，可以了解最新的新闻和信息，以及下载最新的版本。

- Apache Project 下载站点：http://www.apache.org/dist/
- Apache Project 镜像站点：http://www.apache.org/dyn/closer.cgi

5.3.2 启动和停止 Web 服务

Apache 的核心由端口监控程序 httpd 构成，可用脚本/etc/rc.d/init.d/httpd 来运行

使用命令行选项，可启动、停止、重新启动 httpd、或检查 httpd 的状态。

无论何时，当你更改了 httpd 的设置时，都必须重新启动 httpd，以使所作的更改生效。

启动 httpd：

```
# /etc/rc.d/init.d/httpd start
```

停止 httpd：

```
# /etc/rc.d/init.d/httpd stop
```

重新启动 httpd：

```
# /etc/rc.d/init.d/httpd restart
```

检查 httpd 的当前状态：

```
# /etc/rc.d/init.d/httpd status
```

如果 httpd 正在运行，使用 ps 命令可显示与下面类似的应答信息：

```
# ps aux|grep httpd
nobody 351 0.0 3.7 1916 1164 ? S 08:13 0:00 httpd
```

如果你未能见到上述应答信息，就表明未运行 httpd 或未安装 httpd。你可能不得不启动、重新启动、或安装 Apache。

通常情况下，使用其默认设置安装完后，Apache 会直接启动。通过运行在另一台主机上的浏览器，将 IP 地址作为 URL（统一资源定位符）输入，尝试访问 Apache。会见到 Apache 开头的样本 Web 页面。

5.3.3 httpd 配置

httpd 需要四个配置文件。它们各自的通常位置、文件名称和主要目的如下：

文件	目的
/etc/httpd/conf/httpd.conf	针对运行 httpd 端口监控程序的总配置文件
/etc/httpd/conf/srm.conf	针对所要服务的 HTML 文档的细节设置
/etc/httpd/conf/access.conf	访问控制设置
etc/httpd/conf/mime.types/ MIME	MIME（多用途网际邮件扩充协议）文件类型列表

Apache 的一项重要特点在于它具有良好的特性。在上面介绍的合适的配置文件中进行设置，就能利用这些特性。下面，介绍了几项基本内容。

httpd.conf

在文件/etc/httpd/conf/httpd.conf 中，能够发现多种以整体方式作用于 httpd 操作上的设置。在这里，你也可以为 Apache 定义扩展模块。

要想检查 httpd.conf 的内容，可运行：

```
# less /etc/httpd/conf/httpd.conf
```

你应能见到与下面所给出的内容类似的系统响应（部分）：

```
LoadModule mmap_static_module
/usr/libexec/mod_mmap_static.so
LoadModule vhost_aliases_module
/usr/liberec/mod_vhost_alias.so
LoadModule env_module /usr/libexec/mod_env.so
LoadModule config_log_module
/usr/libexec/mod_log_config.so
LoadModule agent_log_module
/usr/libexec/mod_log_agent.so
AddModule mod_mmap_static.c
AddModule mod_vhost_alias.c
AddModule mod_env.c
AddModule mod_log_config.c
AddModule mod_log_agent.c
ServerType standalone
Port 80
HostnameLookups off
User nobody
Group nobody
ServerAdmin root@localhost
```

ServerRoot "/home/httpd/html"

ErrorLog /var/log/httpd/errpr_log

对这些基本设置（指令）的解释如下：

[Load Module] [Add Module]

Apache **的一项优异特性在于它是模块化构造的。该指令告诉** Apache **在扩展模块中进行读取。**

[ServerType]

该指令告诉 Apache（httpd）**，或是以独立模式启动（默认情况），或是作为超级服务器** inetd **的一部分进行启动。如果没有相反方面的特殊理由，建议使用默认方式，即独立模式。**

[Port]

Apache（httpd）**会设置用于接收客户端请求的端口号（默认设置为** 80）**。除非你打算为某一特殊用户运行** Apache**，或允许超级用户**(root)**以外的他人运行** httpd**，否则，你均应使用默认设置，包括端口** 80**，绝大读数服务均使用该默认端口。**

[HostnameLookups]

该指令可以对客户端访问请求的存取日志进行设置，使其使用 IP **地址或主机名。默认设置为"** OFF **"，这表示将记录** IP **地址。建议使用其初始设置。**

[User] [Group]

在这里设置了 httpd **进程的用户和组所有者。在开始情况下，这两者均被设置为了"** nobody **"。之所以采用"** nobody **"设置，是因为可能存在大量的、难以判断的访问数量，而且从安全角度看，对访问权限几乎没有限制。你必须格外小心，正确地配置用户和组许可设置。**

[ServerAdmin]

用来为 Apache（httpd）**系统管理员设置邮件地址。初始值为** root@localhost**。无论何时，当出现任何故障时，会向该地址发送邮件。默认设置的系统管理员地址已很好，但是，当有一个以上的人员负责管理** Web **站点时，在这为所有的** Web **系统管理员指定一个邮递列表，通常情况下会更为方便。**

[ServerRoot]

这是配置文件所在的目录。在默认情况下是/etc/httpd**。建议不要改变这个位置。**

[ErrorLog]

这是保存错误消息的文件。默认情况下，该文件是 logs/error_log**。对该文件的指定是相对于在**[ServerRoot]**指令中指定的目录而言的。如果你打算使用虚拟主机，可为每一个虚拟主机指定单独的错误日志文件。**

[LogFormat] [CustomLog]

在 LogFormat **中指定了存取日志格式，保存访问日志的文件由** CustomLog **指定。如果你打算使用虚拟主机，可为每一个虚拟主机指定单独的日志文件。**

srm.conf

查看/etc/httpd/conf/srm.conf **的内容，可运行：**

```
# less /etc/httpd/conf/srm.conf
```

你将看到与下面类似的内容（只给出了部分）：

```
DocumentRoot /home/httpd/html
UserDir public_html
DirectoryIndex index.html index.shtml index.cgi
FancyIndexing on
ReadName README
HeaderName HEADER
IndexIgnore .??* *~ *# HEADER* README* RCS
AccessFileName .htaccess
TypesConfig /etc/http/cong/mime.types
Alias /icons/ /home/httpd/icons/
ScriptAlias /cgi-bin/ /home/httpd/cgi-bin/
```

对这些基本设置（指令）的解释如下：

[DocumentRoot]

指定了用于组织 HTML **文件的最顶层目录。**

[UserDir]

可被公开的用户目录。

[DirectoryIndex]

指定了将显示的文件名，默认情况下，用于未指定名称的文件。

[Alias]

除了在 DocumentRoot **中指定的外，给出了某一目录的替代名称。**

[ScriptAlias]

指定了保存可执行文件（如 CGI **脚本）的目录的替代名称。**

access.conf

查看 access.conf **文件的内容，可运行：**

```
# less /etc/httpd/conf/access.conf
```

你将看到与下面类似的内容（只给出了部分）：

```
<Directory />
Options None
AllowOverride None
</Directory>
<Directory /home/httpd/html>
Options Indexes Includes FollowSymLinks
```

```
AllowOverride None
order allow, deny
allow from all
</Directory>
<Directory /home/httpd/cgi-bin>
AllowOverride None
Options ExecCGI
</Directory>
```

文件 access.conf **的格式类似于** HTML**。从**<Directory directoryname>**到**</directory>**，指定目录中的设置将被执行。**

在默认情况下，它们被设置为：根目录（/**），**HTML **目录（**/home/httpd/html**），以及** cgi-bin **目录（**/home/httpd/cgi-bin**）。但你也可以添加其它的内容。**

[Options]

主要选项有：

None	**所有选项均无效**
All	**所有选项均有效**
Indexes	**未设置** *srm.conf* **的** DirectoryIndex**（目录索引）时，将以列表方式显示目录。**
ExecCGI	**执行** CGI **脚本的许可**
Includes	**执行** SSI**（服务器端包含）的许可**
IncludesNOEXEC	**给定了执行** SSI**（服务器端包含）的许可，但不允许通过命令**#exec **和**#include **来执行** CGI
FollowSymLinks	**允许使用符号链接**
SymLinksIfOwnerMatch	**只有当目标文件和符号链接的所有者相同时，才允许使用符号链接**

[AllowOverride]

当存取控制文件.htaccess **可用时，可使用它。它能使用的选项如下：**

None	**禁止所有的**.htaccess **选项**
All	**开启所有的**.htaccess **设置**
AuthConfig	**仅允许与认可有关的**.htaccess **设置**
FileInfo	**仅允许与文件格式有关的**.htaccess **设置**
Indexes	**仅允许针对列表的**.htaccess **设置**
Limit	**仅允许针对访问控制的**.htaccess **设置**
Options	**仅允许针对目标目录的**.htaccess **定义**

[order]

为访问许可和拒绝设置决断的先后顺序。可用选项如下：

allow,deny	**按允许、拒绝顺序**
deny,allow	**按拒绝、允许顺序**
mutual-failure	**仅当同时满足和允许和拒绝条件时，才授予许可权限**

[allow from] [deny from]

设置访问许可和拒绝条件。可用选项如下：

all	**允许所有的访问，或拒绝所有的访问请求**
domain name	**允许来自指定域的访问，或拒绝来自指定域的访问**
IP address	**允许或拒绝来自指定 IP 地址的访问**

5.3.4 采用 SSL 的安全站点组织

Turbolinux 7 Server **中的** Apache **包括扩展模块，**mod_ssl**，用它来提供安全套接字协议层（**SSL**）功能。**

如果你打算使用 SSL **来设置安全站点，应去掉可用的** Apache **配置文件的注释（请参见下面的"包含 mod_ssl"），并重新启动** Apache**。此外，为了运行安全服务器，还需要一个已在证书权威部门（**CA**，如** VeriSign**）注册的密钥。请按照这些公认的权威部分给出的步骤，创建并注册密钥。**

5.4.3.1 包含 mod_ssl

要想包含 mod_ssl**，请将文件**/etc/httpd/conf/httpd.bootopt **中下述行前的注释删掉。**

HTTPDOPT=-DSSL/mod_ssl is not included (initial setting)

HTTPDOPT=-DSSL

删除掉注释标记后，重新启动 Apache**。**

/etc/rc.d/init.d/httpd restart

要想检查是否已包括了 mod_ssl**，可使用** Web **浏览器访问：**

https://xxx.xxx.xxx.xxx

其中，xxx.xxx.xxx.xxx **是你自己服务器的** IP **地址。**

5.4.3.2 证书权威机构(CA)

CA **是证书授权机构的缩写，这类机构负责签发数字** ID**，负责签发可在电子邮件、**Web **页面等处作为数字签名使用的数字证书。添加在** Internet **或电子邮件消息上的数字签名可以**

帮助证实：该消息是由声称的作者编写的，而且未被改变。通常情况下，这类证实是通过使用由作者所拥有的公共密钥来执行的。一个数字 ID **就是一个证据，表示该公共密钥是准确的，而且拥有该公共密钥的人员确实存在。**

在美国，这些证书服务是由 VeriSign **提供的。它的** Web **站点是**http://www.verisign.com。

5.4.3.3 加密协议 SSL

SSL**（加密套接字协议层）协议是有** Netscape Communications **开发的。**SSL **协议运行在** TCP/IP**（传输控制协议**/Internet **协议）协议的顶层，除了与** HTTP **一起使用外，还能用在其他方面。其目的就是为了拓展实施了数种协议（如** TELNET、FTP、**网络新闻传输协议** NNTP、**以及轻型目录访问** LDAP）**的应用的使用范围。要想实际使用它，你必须有一个配备了** SSL **的应用程序。**

5.3.5 公共站点设置示例

Apache **通过目录方式来设置访问控制。可以通过文件** access.conf **进行配置，或用放置在你希望控制的目录之下的一个**.htaccess **文件来进行配置。**

例如，如果你只允许来自公司（turbolinux.gr.cn**）内部的主机访问**/home/httpd/html/secret **目录下的文件，那么你的** access.conf **应与下面给出的类似：**

```
<directory /home/httpd/html/secret>
order deny,allow
deny from all
allow from .turbolinux.gr.cn
</directory>
```

如果你打算使用.htaccess **文件，它应与下面的内容类似：**

```
order deny,allow
deny from all
allow from turbolinux.gr.cn
```

5.4 FTP 服务器

FTP 服务器采用了同名协议（FTP）为客户端请求提供服务，可为位于局域网 LAN、企业内部网络 Intranet、或 Internet 上的多台主机提供文件传输服务（下载或上传）。

通常,要想使用 ftp，每个客户端在该 FTP 服务器上都必须拥有一个账户。在一个公共 Internet FTP 站点上，为了满足大量没有“名称”用户的需求，采用了“anonymous”（匿名）或简单的“ftp”作为通用的账户名，允许任何用户登录到 FTP 服务器。

5.4.1 运行 ProFTPD

在 Turbolinux 7 Server 中，FTP 服务是由 ProFTPD 提供的。ProFTPD（专业 FTP 端口监控程序）最初是由“Floody”开发的，目前对它的开发由“MacGyver”（也称为 Habeeb J. Dihu）牵头，很多志愿的自由软件开发人员也投入了其中。ProFTPD 的主 Web 站点是 http://www.proftpd.net。邮递列表位于 http://www.proftpd.org/proftpd-l-archive/。在发行版本中，该程序的名称是 proftpd，全部是小写字母。

5.4.2 Running ProFTPD

能够按下述两种模式中的任何一种运行 ProFTPD：

- 独立模式
- 超级服务器模式

用超级服务器 xinetd 来运行 proftpd 时，没有可供 xinetd 使用的默认的配置文件。开始时，必须以超级用户(root)身份运行 ProFTPD。ProFTPD 使用了标准的 syslog 机制来记录错误。请参见/var/log/messages。

要想在独立模式下启动 ProFTPD，应以超级用户(root)身份，在命令行下简单地键入下述命令即可：

```
# proftpd &
```

如果想检查 proftpd 是否正在运行，可：

```
ps ax | grep proftpd
4296 ? S 0:00 proftpd (accepting connections)
```

如果在进程列表中未出现 proftpd 进程，或是因为未运行它 ;或是因为 proftpd 是从 xinetd 执行的，但在目前没有活动的会话进程。

如果 proftpd 正在运行，可以尝试着用下述命令来使用 ftp：

ftp localhost

Connected to localhost.localdomain.

220 ProFTPD 1.2.1 Server (ProFTPD Default Installation) [sun.dev.cn.tlan]

如果出现了上述消息，就表示 ftp 工作正常。

5.4.3 基本配置

ProFTPD 的配置文件是/etc/proftpd/proftpd.conf。

在这里，我们对 ProFTPD 进行了这样的设置，使其作为带有单个匿名登录帐户的单服务器运行。ProFTPD 服务器是以组“nobody”的“nobody”用户身份运行的。登录到公共服务器的匿名 ftp 客户端将被视为用户“ftp”或“anonymous”（匿名），“anonymous”被设置为用户“ftp”的别名。在你的/etc/group 文件中，在包括系统上所有组的列表中应包含名为“nobody”的组。在你的/etc/passwd 文件中，应包含名为“ftp”的用户。注意，在默认情况下，安装 Turbolinux 7 Server 时，会添加组“nobody”和用户“ftp”。

请使用 cd 命令切换到目录/usr/share/doc/packages/proftpd-1.2.1/sample-configurations/，并查看文件 basic.conf，这是关于 ProFTPD 初始配置的典型示例。如果你打算设置两个匿名目录和一个访客账户，可使用该目录下的示例文件 anonymous.conf。访客账户与匿名账户相同，但需要有效的密码。

在 Turbolinux 7 Server 中，在默认情况下，文件 basic.conf 被简单地重新命名为文件/etc/proftpd/proftpd.conf，以作为 ProFTPD 的初始配置。

ProFTPD 支持多种鉴定方法。默认时采用了 PAM。关于 PAM 的详细信息，请参见文件/usr/share/doc/packages/proftpd-1.2.1-2/README.PAM。

ProFTPD 还具有很多其他特性，如在非标准端口上运行的能力、控制上传/下载率、在 xinetd 下使用、添加另一个匿名登录或访客账户等等，要想了解这些信息，请查看 proftpd 的 的 man page、或访问上面所提到的 Web 站点。

除了配置文件/etc/proftpd/proftpd.conf 外，与 proftpd 有关的其他文件还有：

/usr/sbin/proftpd

/usr/bin/ftpwho

/usr/bin/ftpcount

/usr/sbin/ftpshut

/var/log/xferlog

/var/run/proftpd-[pid]

/var/run/proftpd.pid

/var/run/proftpd-inetd

还能使用 Turbolinux 的工具 serviceboard（请参见第 2-33 页），来启动和停止 proftpd。

第六章　内部网 Intranet 服务器

对于 Intranet 的主机资源共享来说，存在很基本的数种服务。在本章中，我们介绍了一些与下述服务器有关的信息：

• **Samba**：

提供了将 Windows 文件或打印机共享功能，这样，在运行 Windows 的系统和运行 UNIX 的系统之间就能共享诸如文件、打印服务器等资源。

• **Netatalk**：

在 Linux 内核程序中实现了 AppleTalk 协议，能在 Macintosh 和 UNIX 系统之间提供资源共享。

• **Portmapper**：

也称为 portmap，提供了执行 RPC 远程调用所需的支持，能与 NFS 和 NIS 服务器进行通信。

• **NFS**：

网络文件系统，允许在 UNIX 和 Windows 系统之间进行文件共享。

• **NIS**：

在 Intranet 上，针对各种资源的名称和位置的中央数据库更容易实施。NIS 还简化了各种程序对 Intranet 资源的访问。

6.1 Samba

Samba 是一种免费、开放的软件包资源，它实施了用于 UNIX 的服务器信息块（SMB）协议，使用它可将 Windows 系统与 UNIX 系统信息共享。有了 Samba，在 UNIX 系统（如 Linux）和微软的 Windows 系统之间共享资源成为了可能，因此，可以为这两类操作系统提供文件服务、打印服务等。SMB 也被称为公共 Internet 文件系统，LAN（局域网）管理器或 NETBIOS 协议。

此外，通过在 Windows 系统上运行 Samba 客户端程序，就能从 UNIX 系统访问 Windows 资源。（在此，我们不讨论 Samba 客户端程序。要想了解这方面的详细情况，请参阅 smbclient 的 的 man page。关于全部 Samba 套件的介绍，请参见 samba 的 man page）

Samba 是由澳大利亚的程序员 Andrew Tridgell 开发出来的，于 1992 年问世。目前对它的开发由 Samba 团队负责管理。

Turbolinux 7 Server 使用的版本是 Samba-2.2.1。从 Samba 团队的公共 Web 站点，可以了解 Samba 的更多信息以及最新的版本，地址是：http://www.samba.org/。

6.1.1 Samba 套件

Samba 由下述部件组成：

- smbd 服务器端口监控程序，能向 Windows 客户端提供文件共享和打印服务。
- nmbd 提供了 NetBIOS 命名服务和浏览支持。
- smbclient 允许 UNIX 机器将打印件发送到位于 Windows 机器上的打印机处。
- testparm 用于测试 smb.conf 配置。
- testprns 测试文件 printcap 中定义的打印机。
- smbstatus 列出与 SMB 服务器的当前连接,还能显示当前正在运行的 Samba 版本。
- nmblookup 允许从 UNIX 端执行 NetBIOS 名称查询。
- make-smbcodepage 为 smbd 服务器创建 SMB 代码页定义文件。
- smbpasswd 在 Samba 和 Windows 上 SMB 密码。

此外，还有一个基于 HTTP 的配置界面，称为 SWAT（Samba Web 管理工具），该工具允许用户通过浏览器来配置 smb.conf，可以按本地方式，也可以通过 Internet。详情请参见 swat 的 man page。

6.1.2 Samba 启动模式

Samba 可以运行在独立模式下，此时 Samba 端口监控程序会始终处于调用状态；也可以运行在超级服务器模式下（inetd）。此外，当从超级服务器 inetd 启动 Samba 时，通过使用 TCP_Wrapper，能达到更好的安全性。需要指出，Samba 能在下述三种模式下运行：

- 独立模式
- 超级服务器模式
- 带 TCP_Wrapper 的超级服务器模式

独立模式

默认情况下，Turbolinux 7 Server 会在独立模式下启动 Samba。在本手册中，只介绍独立模式。

6.1.3 启动和停止 Samba

Samba 的启动脚本位于/etc/rc.d/init.d/smb。

该启动脚本可使用下述选项：“start”（启动）、“stop”（停止）、“restart”（重新启动）和“status”（状态）。

无论何时，更改了 Samba 配置后，必须重新启动 Samba，才能使所作的更改生效。

启动 Samba：

/etc/rc.d/init.d/smb start

停止 Samba：

/etc/rc.d/init.d/smb stop

重新启动 Samba：

/etc/rc.d/init.d/smb restart

检查 Samba 的状态：

/etc/rc.d/init.d/smb status

你还可以使用 ps 命令来检查 Samba 是否正在运行：

ps aux | grep smb

root 766 0.2 0.2 1764 732 ? S 08:13 0:00 smbd –D

如果你未见到上面所示的响应，Samba 可能未运行，也可能是未安装它。在这种情况下，如果已经安装了 Samba，应重新启动它；或安装 Samba，然后启动之。

6.1.4 Samba 配置

首先，我们将解释服务器端的设置。我们将解释直接修改配置文件的方法。使用名为 SWAT （Samba Web 管理工具）的配置工具也能修改文件 smb.conf，可通过浏览器来使用该工具。关于这点，将在稍后解释。

Samba 是从文件/etc/smb.conf 得到其设置信息的。这是一个文本文件，由几个单元组成，每个单元的开头是一个被方括号“ [] ”括住的名称。该名称将成为文件共享的符号。除［printers］单元外，每个单元都必须与一个目录对应。例如：

[public]

path=/home/samba/public

这意味着，［public］单元中的设置适用于目录/home/samba/public。单元名称［global］、［homes］、以及［printers］保留给系统使用。

[global]　　适用于 Samba 整体的设置

[homes]　　适用于共享主目录的设置

[printers]　　适用于共享打印机的设置

安装 Samba 时，会在目录/etc 下创建 Samba 配置文件 smb.conf。按照安装时给定的情况，smb.conf 会简单地运行 smbd 以及大多数可用的 Samba 特性。但是，出于安全考虑，你应对 smb.conf 进行编辑，反映出使用它的环境。

典型情况下，文件/etc/smb.conf 包含如下内容：

[global]

coding system = euc

client code page = 936

```
workgroup = WORKGROUP
server string = Samba %v
encrypt passwords = Yes
map to guest = Bad User
dns proxy = No
guest account = smbguest

[homes]
comment = %U's home directory
read only = No
browseable = No
[printers]
comment = All Printers
path = /var/spool/samba
print ok = Yes
browseable = No
[private]
comments = Private space; one can write one's own files.
path = /home/samba/private
read only = No
[public]
comment = Public space; anyone can write any files
path = /home/samba/public
guest ok = Yes
read only = No
force group = public
force create mode = 0664
force directory mode = 0775
[tmp]
comment = Read only file space
path = /tmp
guest ok = Yes
```

下面，将分别解释上面所列的每一个代码单元。

[global]（全程）单元

全程单元［global］位于文件 smb.conf 的前面，列出了适用于整个 Samba 的设置。下面，将分别介绍每种设置：

coding system（编码系统）

应使该设置保持其初始的默认值。

client code page（客户端代码页）

应使该设置保持其初始的默认值。

workgroup（工作组）

确定了 Window 网络的 NT 域名，或 Samba 服务器所属的工作组。初始值为“WORKGROUP”。

server string（服务器字符串）

通过已联网计算机上的 Window 客户端进行浏览时，该字符串会出现在“comment”（注释）一栏中。默认值是 Samba %V，其中%V 指的是 Samba 的版本号。对于 Turbolinux 7 Server，%V 的取值为“Samba-2.2.1”。

encrypt passwords（加密密码）

当客户端访问 Samba 服务器时，用于控制是否要检查加密密码。可以将该参数设置为“Yes”或“No”。初始值是“Yes”。

默认情况下，Windows NT 4.0 SP3 和更高的版本、以及 Windows 98 要求使用加密密码。因此，必须将参数设置为“Yes”。稍后，我们将给出有关配置加密密码的更多信息。

map to guest（映象到访客）

该参数会告诉 smbd，当遇到来自某一用户的请求，而且该用户与已注册的 UNIX 用户账户不完全匹配时，应采取什么行动。可以取下面所列的三个值之一。初始取值是“Bad User”（不良用户）。

Never（从不）	拒绝使用无效密码的登录请求
Bad User（不良用户）	如果用户名无效但密码有效，将被视为访客登录，并被映射到“guest account”（访客账户），关于这点，将在稍后解释。
Bad Password（不良密码）	如果用户名有效但密码无效，将被视为访客登录，并被映射到“guest account”（访客账户），关于这点，将在稍后解释。

你应将该参数设置为“Never”或“Bad User”。使用“Bad Password”时要当心，这是因为，错误地输入了自己密码的用户将以“guest”身份登录。不会给出错误信息，因此，用户很可能会纳闷为什么不能访问他（或她）自己的文件和目录。

dns proxy（DNS 代理）

当无法找到 NetBIOS 名称时，该设置会指出是否要将该名称作为给定的 DNS 名称对待。该参数必须是“Yes”或“No”。默认值是“No”。

guest account（访客账户）

在该单元中，如果将参数设置为 guest ok＝Yes，那么它就是用来访问服务的用户名。默认值是 smbguest。

主目录单元[homes]

本单元用于保存适用于用户主目录的设置。

comment（注释）

对这里所给出的目录的一些解释。通过已联网计算机上的 Window 客户端浏览该目录时，该字符串会出现在“comment”（注释）一栏中。默认值是“%U 的主目录”，其中，变量%U 将被 Samba 服务器上的登录名取代。例如，如果用户的名称是“pat”，那么将显示“pat

的主目录”

read only（只读）

用于决定用户主目录是否是只读的，或是否也允许写入。该参数必须是“ Yes ”或“ No ”，默认值为“ No ”。

browseable（可浏览）

通过已联网计算机上的 Window 客户端浏览该目录时，该字符串会出现在“ comment ”（注释）一栏中。该参数必须是“ Yes ”或“ No ”，默认值为“ No ”。

打印机单元[printers]

本单元用于保存适用于共享打印机的设置。

comment（注释）

对这里所给出的打印机的一些解释。通过已联网计算机上的 Window 客户端浏览该目录时，该字符串会出现在“ comment ”（注释）一栏中。默认值是“ All Printer ”（所有的打印机）。

path（路径）

指定了打印缓冲目录的完整路径，默认值是“ /var/spool/samba ”。

print ok（打印 OK）

用于决定是否允许用户对打印缓冲文件进行写入操作。该参数必须是“ Yes ”或“ No ”，默认值为“ Yes ”。

browseable（可浏览）

通过已联网计算机上的 Window 客户端浏览该目录时，用于决定是否显示打印机。该参数必须是“ Yes ”或“ No ”，默认值为“ No ”。

私有单元[private]

在本单元中给出了一个示例，指出了当你打算共享私人目录时，可使用些什么。该单元不是必需的，但在很多场合，可能需要它。

该单元的名称就是共享目录的名称。在这里，将共享目录设置为“ public ”。

comment（注释）

包含对目录的一些解释。通过已联网计算机上的 Window 客户端浏览该目录时，该字符串会出现在“ comment ”（注释）一栏中。默认值是“ Private space; one can write one’s own files ”（私人空间，某人能更改其自己的文件）。

path（路径）

指定了共享目录的完整路径，默认值是“ /home/samba/private ”。

read only（只读）

用于决定用户主目录是否是只读的，或是否也允许写入。该参数必须是“ Yes ”或“ No ”，默认值为“ No ”。

公共单元[public]

在本单元中给出了一个示例，指出了当你打算共享公共目录时，可使用些什么。该单元不是必需的，但在很多场合，可能需要它。

comment（注释）

包含对目录的一些解释。通过已联网计算机上的 Window 客户端浏览该目录时，该字符串会出现在“comment”（注释）栏中。默认值是“Public space; anyone can write any files”（公共空间，任何人都能写入任何文件）。

path（路径）

指定了共享目录的完整路径，默认值是“/home/samba/public”。

guest ok（访客 OK）

用于决定是否允许来自访客账户的访问。如果允许，那么来自某些用户账户的人员就能访问它，这些用户账户是在全程单元［global］的“guest account”参数中设置的。

read only（只读）

用于决定用户主目录是否是只读的，或是否也允许写入。该参数必须是“Yes”或“No”，默认值为“No”。

force group（强制组）

对在该目录中创建的文件和目录，强行设置为组所有权。默认值是“public”。

force create mode（强制创建模式）

在这里，你可以为在该目录中创建的文件指定强制的许可设置，默认值是 644。

force directory mode（强制目录模式）

在这里，你可以为在该目录中创建的目录指定强制的许可设置，默认值是 755。

临时单元[tmp]

在本单元中给出了一个示例，指出了当你打算共享临时目录（只读）时，可使用的配置。该单元不是必需的，但在很多场合，可能需要它。

comment（注释）

包含对该目录的一些解释。通过已联网计算机上的 Window 客户端浏览该目录时，该字符串会出现在“comment”（注释）一栏中。默认值是“Read only file space”（只读文件空间）。

path（路径）

指定了共享目录的完整路径，默认值是“/tmp”。

guest ok（访客 OK）

用于决定是否允许来自访客账户的访问。如果允许，那么来自某些用户账户的人员就能访问它，这些用户账户是在全程单元［global］的“guest account”参数中设置的。

6.1.5 加密密码

自 Windows NT SP3 以后，以及在 Windows 98 中，采用了加密密码作为默认设置，而不

是以前网络上常见的明码文本密码。但是，由于这些加密密码与 UNIX 系统不兼容，使得无法进行相应的访问。因此，有必要为 Samba 服务器专门创建一个密码文件。要想开启加密密码功能，就应在全程单元［global］中将参数设置为 encrypt password=Yes。

对于使用加密密码而言，Samba 服务器需要一个名为 smbpasswd 的密码文件。要想使用加密密码，应以超级用户(root)身份登录，并尊序下面给出的指导步骤。

创建文件 smbpasswd

在目录/etc 下，创建一个名为 smbpasswd 的空文件。只有超级用户才能对该文件进行读取和写入操作。

```
# touch /etc/smbpasswd
# chmod 600 /etc/smbpasswd
```

用户注册

对于要注册到文件 smbpasswd 的用户来说，他（或她）必须注册到系统上。在这里，我们以用户“pat”为例。

\# **useradd pat**

\# **smbpasswd -a pat**

New SMB Password : ***password***

Repeat New SMB Password : ***password***

Added user pat

Password changed for user pat

要想将一位已注册的用户写入（附加）到文件 smbpasswd 中，可运行命令：

```
# cat /etc/passwd | mksbpasswd.sh >> /etc/smbpasswd
```

将用户添加到文件 smbpasswd 后，应更改用户的密码。

#smbpasswd -a -e pat

user pat enabled

一旦更改完成，请重新启动 Samba。

6.1.6 文件和打印机共享

对于文件和打印机共享来说，有四种设置其格式的方式。对于全程单元［global］中的参数 security，你必须决定为它设置下面四个取值中的哪一个。参数 security 或许是文件 smb.conf 中最重要的设置。这四个取值是：

- share（共享）
- user（用户）
- server（服务器）
- domain（域）

Share（共享）

共享是按目录和设备而设置的。它们与 Windows 95 中的共享设置具有相同的等级。未

注册到 Samba 服务器的用户仍能访问它们。从安全的角度考虑，这是最“仁慈”的配置。

User（用户）

共享是按用户设置的。其识别由 Samba 来完成，因此，能够获得访问权限的用户必须事先注册到 Samba 服务器上。不仅如此，对于来自 Windows 98 以及 NT SP3 和更高版本的访问来说，还需要使用加密密码。关于更详细的信息，请参见“加密密码”。

Server（服务器）

该配置与上面介绍的“user”（用户）相仿，唯一的差别是，鉴定不是由 Samba 服务器，而是由另一台 Windows NT 服务器完成的。能够获得访问权限的用户必须事先注册到另一台 Windows NT 服务器上。在这种情况下，由于 Samba 服务器被视为 Windows Nt 服务器的一个客户端，因此，你必须确保自己至少拥有一个附加的 Windows NT 客户端许可证书。

Domain（域）

该配置与上面介绍的“user”（用户）相仿，唯一的差别是，Samba 服务器被指定为已存在的 Windows NT 域的一名成员。简而言之，鉴定并不是由 Samba 服务器完成的，而是由 Windows NT 服务器（域控制器）实现的。用户要想获得访问权限，就必须注册到这个域上。在这种情况下，由于 Samba 服务器被视为 Windows Nt 服务器的一个客户端，因此，你必须确保自己至少拥有一个附加的 Windows NT 客户端许可证书。

正如前面所阐述的那样，当未以明确设置参数 security 时，会假定 security=user。

6.1.7 测试设置

通过运行命令 testparm，你可以检查是否正确构造了配置文件：

```
# testparm
Load smb config files from /etc/smb.conf
Processing section "[homes]"
Processing section "[printers]"
Processing section "[private]"
Processing section "[public]"
Processing section "[tmp]"
Loaded services file OK.
Press Enter to see a dump of your service definitions
```

在该点，显示会暂停下来，按下回车键即可查看测试结果。

6.1.8 通过 SWAT 进行配置

SWAT（Samba Web 管理工具）通过 Web 浏览器对 Samba 进行配置。SWAT 是 Samba 软件包的一部分，会自动地与 Samba 软件包一起被安装到系统。

SWAT 设置

要想在超级服务器模式下运行，就应对文件/etc/xinetd.d/swat 进行编辑。将变量“disable”

的取值更改为“no”，保存文件，并重新启动 xinetd。

/etc/rc.d/init.d/xinetd restart

如何使用 SWAT

使用 SWAT 时，文件/etc/smb.conf 的初始状态会被覆盖。如果你打算保存该配置文件的先前状态，请备份它。

一旦完成了准备工作，可运行 Web 浏览器并连接到 SWAT。初始情况下，SWAT 将被设置为使用端口 901。如果打算以本地方式访问它，可使用 URL 地址 http://localhost:901/。

一旦你设置了 IP 地址和端口号，也能以远程方式访问 SWAT。

当打开页面时，会要求身份识别。在这，你可以输入系统管理员的账户和密码。正常情况下，应键入超级用户(root)及其密码。至此，会出现 Samba 主页。

在主页上方，包含下述图标，这些图标与对应的配置屏幕相链接。

- (HOME) （主页）
- (GLOBALS) （全程）
- (SHARES) （共享）
- (PRINTERS) （打印机）
- (STATUS) （状态）
- (VIEW) （查看）
- (PASSWORD) （密码）

(HOME)（主页）

这是 SWAT 的主页，从这里，你可以跳至各帮助屏幕，或单独的配置屏幕。

(GLOBALS) （全程）

适用于文件 smb.conf 的全程单元［global］设置。选择“Details”（细节）选项可了解详细内容。选择每个配置条目左侧的“Explantion”（解释）选项可看到 SWAT 的帮助文档。选择“Reset”（重置）选项，可将所有的设置重新设为默认值。对于每一个条目，都有一个“Return to previous setting”（返回上次设置）按钮，使用该按钮，可将该条目返回到它上次的设置。更改完设置后，选择“Change Settings”（变更设置）选项，将新设置合并到文件 smb.conf。

(SHARES) （共享）

要想设置共享目录，可从按钮列表选择 smb.conf 单元，并选择“Shares”（共享）。这是，将显示该单元的内容。如果打算删除共享资源，请从按钮列表选择单元名称，并选择“Remove Shares”（删除共享）。选择“Create New Shares”（创建新的共享资源），可创建新的共享单元。

(PRINTERS) （打印机）

要想设置共享打印机，可从按钮列表选择 smb.conf 单元，并选择“Shares”（共享）。这是，将显示该单元的内容。如果打算删除共享资源，请从按钮列表选择单元名称，并选择“Remove Shares”（删除共享。注意，对于名称是以星号“*”开头的那些打印机来说，不会自动将它们从文件/etc/printcap 中删除）。选择“Create New Printers”（创建新的打印机），

可创建新的打印机单元。

(STATUS) （状态）

该按钮能显示 smbd 的状态。此外，更改了设置以后，你可以在这里启动/停止 Samba。

(VIEW) （查看）

使用该按钮，可查看文件 smb.conf 的当前内容。

(PASSWORD) （密码）

使用该按钮，可注册用户并更改密码，就象在 smbpasswd 中那样。

6.1.9 Windows 共享和 Macintosh 共享的共存

Samba 和 Netatalk 以及它们各种相应的设置和操作可以共存，不会出现问题。

使用 Netatalk 的文件共享功能，你可以创建并共享本地 Macintosh 文件和目录。你也可以对这些文件和目录进行设置，使得其他平台不能看到它们。

将下面两行内容添加到文件/etc/smb.conf：

```
veto file = /.AppleDesktop/NetworkTrashFolder/.AppleDouble/
delete veto files = true
```

通过“delete veto files=true”设置，可以删除由“veto”（否决）文件设置的文件。

6.2 Netatalk

Netatalk 是由位于密执安大学的研究系统 UNIX 组（RSUG）开发的。从他们的公共 Web 站点，可了解更多的 Netatalk 信息，并获得最新的补丁程序。可以从 RSUG 的下载站点下载 Netatalk 源代码，其网址是 http://www.umich.edu/~rsug/netatalk/。

Netatalk 在 Linux 内核程序上实施了 AppleTalk 协议，并能提供多种功能特性，如路由、文件服务器、以及打印服务器。在 AppleShare 环境下使用 Netatalk，就能从 Macintosh 系统访问位于 Linux 系统上的文件和打印机。在这些功能中，DDP 是在 Linux 内核程序中实现的，但其他协议是作为端口监控程序和命令来实施的。

EtherTalk 阶段 I 和 II

DDP	数据报递送协议
RTMP	路由表维护协议
NBP	命名编联协议
ZIP	地区信息协议
AEP	AppleTalk 回应协议
ATP	AppleTalk 交易协议
PAP	打印机访问协议
ASP	AppleTalk 会话协议
AFP	AppleTalk 过滤协议

6.2.1 Netatalk 部件

Netatalk 的主要部件有：

端口监控程序	配置文件	配置内容
/usr/sbin/atalkd	/etc/atalk/atalkd.conf	AppleTalk 设置
/usr/sbin/afpd	/etc/atalk/AppleVolumes.default	文件共享设置
	/etc.atalkAppleVolumes.system	文件共享设置
/usr/sbin/papd	/etc/atalk/papd.conf	文件共享设置

[atalkd]

Netatalk 服务器是 atalkd，它能提供与借助 TCP/IP 协议组的 routed 端口监控程序相同的功能。端口监控程序 atalkd 实施了 RTMP、NBP、ZIP 和 AEP 协议。它的配置文件是 atalkd.conf。

[afpd]

端口监控程序 afpt 实施了 AFP 协议。使用该端口监控程序，就能与 Macintosh 共享 UNIX 文件系统。它的配置文件是 AppleVolumes.default 和 AppleVolumes.system。

[papd]

端口监控程序 papd **实施了** PAP**（打印机访问）协议。使用它，你可以从** Macintosh **机器将内容发送到** Turbolinux **服务上，并使用** Turbolinux **的** AppleTalk **打印机将其打印出来，在这里，假定你已经有了必要的** PostScript **打印机。如果你使用的是非** PostScript **打印机，就有必要使用不同的打印机驱动程序，因此必须有** ghostscript**（幽灵脚本）或类似的实用工具**(**默认已经安装**)。Papd **的配置文件是** papd.conf。

6.2.2 启动和停止 Netatalk

Netatalk **的启动脚本是**/etc/rc.d/init.d/atalk。

该启动脚本可用的选项是：" start "**（启动）、**" stop "**（停止）、**" restart "**（重新启动）和**" status "**（状态）。**

一旦更改了 Netatalk **的设置，就必须重新启动** Netatalk**，才能使所作的更改生效。**

启动 Netatalk**：**

```
# /etc/rc.d/init.d/atalk start
```

停止 Netatalk**：**

```
# /etc/rc.d/init.d/atalk stop
```

重新启动 Netatalk**：**

```
# /etc/rc.d/init.d/atalk restart
```

要想检查 Netatalk **的当前状态，可运行：**

```
# /etc/rc.d/init.d/atalk status
```

使用 ps **命令，可以验证** Netatalk **是否正在运行，如下所示：**

```
# ps aux | grep atalk
root 766 0.2 0.2 1764 732 ? S 08:13 0:00 atalkd
```

如果你未能见到与上面所给出的内容类似的信息，那么或是因为 Netatalk **未运行，或是未安装** Netatalk。**在这类情形下，需要安装、启动、或重新启动** Netatalk。

如果你不能运行 Netatalk**，可使用命令** lsmod **检查是否已加载了** AppleTalk **模块：**

```
# lsmod
Module          Size            Used by
appletalk       17504   14      (autoclean)
nls_iso8859-1   2020    1       (autoclean)
isofs           17208   1       (autoclean)
epic100         10724   1       (autoclean)
st              25440   0
ncr53c8xx50344  1
```

如果未出现 AppleTalk **模块，就有必要以手动方式使用下述命令来加载该模块：**

```
# modprobe appletalk
```

6.2.3 Netatalk 设置

在这一部分中，介绍了当你打算在 Macintosh 机器上使用 Netatalk 来共享文件和打印机时，针对文件服务器和打印服务器所作的 Linux 配置。在该部分中，首先首先将解释服务器（TurboLinus＋Netatalk 端）。然后将解释客户端（Macintosh 端）。

针对文件共享的 Linux 端（服务器）设置

用于实现文件共享的端口监控程序是 afpd。它的配置文件是 AppleVolumes.default 和 AppleVolumes.system。

AppleVolumes.default	使 AppleShare 卷成为公共目录的设置
AppleVolumes.system	应用于文件扩展和文件类型上的设置

这两个文件决定了：将 Turbolinux 服务器上的文件和目录按 AppleShare 卷的形式设置为公共的方式。它们是由公共目录设置和文件定义来组织的。

公共目录设置（AppleVolumes.default）

Netatalk RPM 软件包会在预先定义好的位置处安装标准的配置文件。这里，给出了标准 AppleVolumes.default 文件的内容：

```
# This file looks empty when viewed with "vi". In fact,
# there is one '~', so users with no AppleVolumes file in
# their home directory get their home directory by default
# volume format:
# path [name] [casefold=x] [codepage=y] [poptions=z,l,j]
[access=a,@b,c,d]
# casefold options:
# tolower lowercase names in both directions
# toupper uppercases names in both directions
# xlatelower client sees lowercase, server sees uppercase
# xlateupper client sees uppercase, server sees lowercase
#
# access format:
# user1,@group,user2 restricts volume to listed users/groups
#
# miscellaneous options
# prodos make compatible with AppleII clients.
# crlf enable crlf translation for TEXT files.
#
# codepage=filenameload filename from nls directory.
#
~
```

在上面给出的文件内容中，任何以符号“#”开头的行均是注释行，均将被忽略。事实上，只有最后一行，即包含代字符“~”的行才会被读取。

代字符“~”表示每位用户的主目录。在这个不是很常见的示例中，每位登录的用户都能看到他自己的主目录。如果不希望将每位用户的主目录公开，应删除代字符“~”，或将该行设为注释行。

要想公开除用户主目录外的所有目录，可作如下设置：

[Full path to the directory you want to make public] [Macintosh volume name]

这里给出了一个例子，介绍了借助卷名 MACPUB，从 Macintosh 端访问 Linux 服务器端目录/home/public 的方法。

将下行内容添加到文件 AppleVolumes.default 上：

/home/public MACPUB

Macintosh所使用的特殊文件和目录

一旦 Netatalk 公开了目录，要想访问这些目录，必须在这些目录中创建下面这两个文件：

AppleDesktop Macintosh 桌面文件

AppleDouble Macintosh 资源文件

密码和访问许可

对于文件共享来说，密码和访问许可十分重要。但是，使用了 Netatalk 时，能将 Linux 服务器上的密码和访问许可递送到 Macintosh 端。

当你打算更改许可设置时，正常情况下，可以使用 Linux 服务器上的 chmod 命令。例如，如果你打算限制对目录/home/public 的读取，应以超级用户身份登录到 Linux 服务器，然后运行下述命令：

```
# chmod 755 /home/public
```

定义文件类型

用于定义文件类型的格式如下：

[extension] [file type] [application or client]

作为一个特殊示例，对 HTML、PDF 和 MS Word 文件的定义如下：

.html TEXT MOSS HyperText Markup Language (HTML)

.pdf PDF CARO Portable Display Format (Adobe Acrobat)

.doc WDBN MSWD Word Document

下面是一个实际例子，给出了典型 AppleVolume.system 文件的一部分：

.	"TEXT"	"ttxt"	ASCII Text
.sty	"TEXT"	"*TEX"	TeX Style
.psd	"8BPS"	"8BIM"	PhotoShop Document
.pxr	"PXR	"	"8BIM" Pixar Image
.sea	"APPL"	"????"	Self-Extracting Archive
.apd	"TEXT"	"ALD3"	Aldus Printer Description
.pm3	"ALB3"	"ALD3"	PageMaker 3 Document
.pm4	"ALB4"	"ALD4"	PageMaker 4 Document
.pt4	"ALT4"	"ALD4"	PageMaker 4 Template
.pm5	"ALB5"	"ALD5"	PageMaker 5 Document
.pt5	"ALT5"	"ALD5"	PageMaker 5 Template
.pdx	"TEXT"	"ALD5"	Printer Description
.ppd	"TEXT"	"ALD5"	Printer Description
.dl	"DL	"	"AnVw" DL Animation
.gl	"GL	"	"AnVw" GL Animation

.url	"AURL"	"Arch"	URL Bookmark
.zoo	"Zoo	"	"Booz" Zoo Archive
.pdf	"PDF	"	"CARO" Portable Document Format
.h	"TEXT"	"CWIE"	C Include File
.hp	"TEXT"	"CWIE"	C Include File
.hpp	"TEXT"	"CWIE"	C Include File
.c	"TEXT"	"CWIE"	C Source
.cp	"TEXT"	"CWIE"	C++ Source
.cpp	"TEXT"	"CWIE"	C++ Source
.class	"Clss"	"CWIE"	Java Class File
.java	"TEXT"	"CWIE"	Java Source File

.....剩余略.....

打印机共享设置

要想通过 AppleTalk 从 Macintosh 使用 Linux 打印机，可以使用 papd。如果你不打算共享打印机，就没有必要运行 papd。用于 papd 的配置文件是/etc/atalk/papd.conf。

papd.conf 的语法与 Linux 上的 printcap(5)相同：

```
<share>:
:pr=<printer>:op=<operator>:pd=<filename>
```

其中，<share>可以是任何打印机的名称，从 Macintosh 端可看到此名称。

配置参数（属性）以及它们的意义如下：

Pr	Lpd 打印机名称
Op	当创建了 lpd 缓冲文件时的所有者
Pd	PDF 文件的路径

请注意下面两点：

- 由 pr 设置的名称必须是已注册到文件/etc/printcap 中的打印机名称。
- 由 op 设置的用户名必须是在 Linux 服务器上拥有账户的用户，而且是可以使用指定打印机的用户。

配置示例

在下面这个示例中，为了能从 Macintosh 端看到 Linux 上的打印机名称，将打印机名称设置为了 ps，并将缓冲文件的所有者设置为超级用户(root)“root”。

```
Linux Printer:\
:pr=ps:op=root;\
:pd=/usr/share/lib/ppd/HPLJ_4M.PPD:
```

共享多台打印机也是可能的，在这种情况下，必须将对应的设置田间到文件 papd.conf 中。

由于 Netatalk RPM 软件包会安装初始化文件，因此，会显示并确认用于 papd.conf 的默认设置。

```
# Attributes are:
#
```

```
# Name Type Default Description
# pd str ".ppd" Pathname to ppd file.
# pr str "lp" LPD printer name.
# op str "operator" Operator name, for LPD spooling.
#
# Some examples:
# On many systems (notably not Solaris), no papd.conf is required,
# since papd shares the same defaults as lpd.
#
# A simple example:
#
# terminator:
# :pr=lp:op=wes:
# :pd=/usr/share/lib/ppd/HPLJ_4M.PPD:
#
# Note also that papd.conf can list several printers.
```

如果你在 Linux 服务器端上更改了设置，就必须重新启动 Netatalk。在前面，我们已经介绍了重新启动的步骤。

Macintosh 客户端设置

不需要进行特别的设置。打开选择器并选择“AppleShare”，并从计算机名称列表中选择 Linux 服务器。当问及用户名和密码时，请输入你在该 Linux 服务器上的用户名和密码。

运行检查

从 Machintosh 端执行 Netatalk 运行检查十分简单。打开选择器并选择“AppleShare”。如果你看到了 Linux 服务器的计算机名称，就表示 Netatalk 运行正常。接下来，在 Linux 上进行了共享设置以后，如果能够从 Macintosh 端访问 Linux 目录，就表示已经正确配置了 Macintosh。

6.2.4 Portmapper (portmap)

Portmap 服务器能将 RPC（远程过程调用）程序号转换为 DARPA 协议号。要想使用诸如 NIF 和 NFS 等服务器，就需要运行 portmap，在 portmap 中实施了 RPC（远程过程调用）。

在 Turbolinux 7 Server 环境下，不会自动启动 portmap。首先，你必须使用 serviceboard 来配置它。

启动脚本可用的选项有“ start ”（启动）、“ stop ”（停止）、“ restart ”（重新启动）、“ status ”（状态）和“ reload ”（重新加载）。

一旦你更改了 portmap 的设置，要想使所作的更改生效，就必须重新启动 portmap。

要想启动 portmap，可运行：

#/etc/rc.d/init.d/portmap start

要想停止 portmap，可运行：

#/etc/rc.d/init.d/portmap stop

要想重新启动 portmap，可运行：

#/etc/rc.d/init.d/portmap restart

要想检查 portmap 的当前状态，可运行：

#/etc/rc.d/init.d/portmap status

尽管 portmap 十分方便，但从安全的角度看，它也存在很多问题。对于默认安装的 portmap 来说，会用到 xinetd 访问控制库。在 Turbolinux 7 Server 的初始设置下，portmap 不会接受来自其他客户端的请求。正因为如此，仅靠运行 portmap，并不能使用 NFS 和 NIS。你还需要修改访问控制文件/etc/hosts.allow。

在下面给出的示例中，允许来自.turbolinux.gr.cn 域或 192.168.0.1 的机器进行访问

portmap: .turbolinux.gr.cn

portmap: 192.168.0.1

无需重新启动 portmap 就能反映出访问控制文件中的变化。

要想了解如何定义访问控制，请参见 “ 访问控制 ”一节。

注意：

portmap 服务器不是从 xinetd 启动的，但 portmap 本身能够参照文件/etc/hosts.allow 和 /etc/hosts.deny。注意，portmap 不是从超级服务器启动的。

6.3 NFS

使用 NFS**（网络文件系统），你就能在连接到网络上的多台主机之间共享文件。大多数** UNIX **均支持** NFS**，在** UNIX **系统上，这是传输文件的一条便利途径。此外，通过一些附加的软件，可以在不同于** UNIX **的操作系统支持** NFS**，并能在众多计算机之间透明地传输文件。**

在 Turbolinux 7 Server **上，你可以安装** knfsd**，提升** NFS **服务器的性能，传统情况下，** NFS **是运行在用户层次上。**

要想使用 NFS**，就必须在服务器端和客户端配置** NFS**。在服务器端，可以对基本的配置文件**/etc/exports **进行编辑，然后运行该端口监控程序。在客户端，你必须加载那些被导出的目录（公开它们）。**

6.3.1 启动和停止 NFS

NFS **的启动脚本是**/etc/rc.d/init.d/nfs**。启动脚本可用的选项有**“start”**（启动）、**“stop”**（停止）和**“restart”**（重新启动）。**

一旦你更改了 NFS **的设置，要想使所作的更改生效，就必须重新启动** NFS**。**

启动 NFS**：**

#/etc/rc.d/init.d/nfs start

停止 NFS**：**

#/etc/rc.d/init.d/nfs stop

重新启动 NFS**：**

#/etc/rc.d/init.d/nfs restart

要想查看 NFS **的状态，可**

#/etc/rc.d/init.d/nfs status

要想重新加载 NFS**，可：**

#/etc/rc.d/init.d/nfs reload

运行命令 ps **可检查** NFS **的当前状态。如果** NFS **正在运行，你将见到与下面所示内容类似的信息：**

ps aux | grep nfs

root 766 0.2 0.2 1764 732 ? S 08:13 0:00 nfsd

如果你未能见到类似上面的响应，就表示 NFS **未运行，或者是未安装** NFS**。在这类情形下，需要启动、重新启动、或安装** NFS**。**

6.3.2 NFS 服务器设置

在本部分中，我们将详细介绍各种与使用 NFS 服务器有关的设置情况。

/etc/exports 设置

在文件/etc/exports 中，你可以指定主机、用户、公共目录，可被访问的资源、以及访问许可等。文件/etc/exports 中的每一行均采用了下述格式：

[directory name] [host name (options)]

这里，“directory name”指的是你打算与完整 UNIX 路径一起导出的目录名称。“host name”可采用 FQDN（正式域名）或 IP 地址格式。有很多可用的选项，这里只介绍的主要的一些。要想了解更多的信息，请运行：

man exports

这里给出了部分选项的列表：

Ro	将文件许可设置为只读
Rw	将文件许可设置为可读、可写
Root_squash	来自客户端的超级用户(root)访问将被映射为匿名（nobody）
no_root_squash	允许来自客户端的超级用户(root)访问作为超级用户(root)
all_squash	所有的访问均被视为来自“nobody”的访问
anonuid=uid	与 root_squash 或 all_squash 选项一起使用，映射为匿名用户 ID
anongid=gid	与 root_squash 或 all_squash 选项一起使用，映射为匿名组用户 ID

注意：

通过逗号将选项分隔开来，可以一次指定多个选项。但是，如果在选项和命令之间插入空格，可能会导致无法预料的结果。

下面，给出了文件/etc/exports 的一个示例：

/usr *.turbolinux.gr.cn(ro)

/home/you test (rw,all_squash,anonuid=150,anongid=100)

/home/samba (ro,all_squash)

在第 1 行中，允许 turbolinux.gr.cn 域下的所有机器读取/usr 下的所有内容。

在第 2 行中，允许名为 test 的机器对/home/you 进行读写操作。不管实际用户是谁，多访问作了这样的设置，UID（用户 ID）被设为 150，GID（组 ID）被设为 100。

在第 3 行中，请注意未指定主机名。这表示允许所有的主机读取（不可写）/home/samba。所有访问均是通过“nobody”账户进行的。

运行服务器

运行 NFS 服务器前，请检查是否已经使用了恰当的设置运行了 portmap。

与其他服务器一样，NFS 是与 init 脚本一道启动的。由于在 Turbolinux 7 Server 中，不会在默认情况下运行 NFS，因此你必须使用 chkconfig 或 serviceboard 对其进行配置，以便在重新启动后，能作为端口监控程序启动 NFS。

NFS 服务器运行检查

使用 exportfs 可检查 NFS 导出的状态。（命令 exportfs 还有其他用处，详情请参见 exportfs 的 man page）。

例如，使用上面所给出的/etc/exports 配置示例，exportfs 的输出结果与下面给出的类似：

```
# exportfs
/usr *.Turbolinux.ge.jp
/home/your test
/home/samba <world>
```

使用命令 showmount，可以显示在单独客户端上加载的目录。例如，如果在主机 test2.turbolinux.gr.cn 上加载了/usr，将见到：

```
# showmount -a
All mount points on cadiz.calleprivada:
test2.turbolinux.gr.cn:/usr
```

6.3.3 客户端设置

NFS 服务器可能会拥有大量的和各种各样的客户端，但在这里，我们仅介绍运行 Linux 的客户端。

一般而言，客户端能够使用 mount 命令来加载被 NFS 服务器导出的目录。例如，要想将 NFS 服务器（nfssvr）的/usr 目录加载到/mnt/usr，可：

```
# mount -t nfs nfssvr:/usr /mnt/
```

通过编辑文件/etc/fstab，可以直接使用 mount，而没有必要每次都给出所有的命令行选项。

例如，可以将下行内容添加到你的/etc/fstab 文件中。

```
nfssvr:/usr /mnt/usr nfs noauto,rw
```

然后，就可以仅使用命令 mount 来执行加载操作。

```
# mount /mnt/usr
```

这是一个相当简单的例子。在实际使用过程中，可以在命令行上给出一些选项，或者将这些选项编辑到文件/etc/fstab 中。常用的一些选项有“rsize”（读容量）、“wsize”（写容量）、“hard”（硬）、“soft”（软）和“timeo”（超时）。

rsize	指定读缓冲区的大小（默认值是 1024）。尽管存在上限，但该容量越大、传输速度就越快。
Wsize	指定写缓冲区的大小（默认值是 1024）。
hard	即使当服务器宕机时，连接请求仍能继续。当服务器宕机时，在控制台上会出现消息 " server not responding "（服务器未应答）。
soft	当有一段时间未收到来自 NFS 服务器的响应时，允许设置内核程序超时
Timeo	设置了 soft 时，用来指定超时的长度

下面给出了一个使用上述选项/etc/fstab 示例：

```
nfssvr:/usr /mnt/usr nfs noauto,rw,rsize=8192,wsize=8192,soft,timeo=1000
```

在本例中，读缓冲区和写缓冲区均被设为 8192 字节，当服务器的未响应时间超过 1000 毫秒，超时开始。

6.3.4 安全

NFS 是一种包含了很多元素的服务器，对于系统安全来说，这些元素可能存在问题，正因为如此，建议你在位于防火墙后面的本地网络上使用它。而且，你还应仔细审查对文件/etc/exports 的访问许可。此外，在应用 portmap 访问控制时，还应有一个恰当的安全策略，仅接受来自特定客户端的 RPC 调用。

6.4 NIS

NIS（网络信息服务）用于共享与网络上的计算机有关的信息，如登录名称、密码、主目录（/etc/passwd）和用户组（/etc/group）。

6.4.1 服务器和客户端共同的设置

对于 NIS 服务器和 NIS 客户端来说，有些设置是相同的。下面，我们将讨论这些设置。

运行 portmap

要想运行 NIS，就必须运行 portmap。正常情况下，当引导 Turbolinux 7 Server 时，不会启动 portmap。使用下述命令，可检查 portmap 是否正在运行：

```
# /etc/rc.d/init.d/portmap status
```

如果 portmap 正在运行，系统响应是：

```
portmap (pid 168) is running...
```

另外，Turbolinux 7 Server 中所包含的 portmap 会参考/etc/hosts.allow 和/etc/host.deny 文件，因此，必须将下行内容添加到文件/etc/hosts.allow 中：

```
portmap : 192.168.1.0/255.255.255.0 : allow
```

NIS 域设置

可以使用命令 domainname，或通过编辑文件/etc/sysconfig/network 来配置 NIS。执行该任务时，可运行：

```
# domainname [domainname]
```

或将下行内容添加到文件/etc/sysconfig/network 中：

```
NISDOMAIN = [domainname]
```

注意：

所设置的 DNS 域名应有别于 NIS 域名

6.4.2 服务器设置

请检查文件/etc/ypserv.conf 是否可用。

接下来，创建文件/var/yp/securenets。通过设置网络掩码“netmask”和网络地址“network address”，指定 NIS 网络的适用范围。添加下行内容：

```
[netmask] [network address]
```

在 netmask 字段中指定与网络地址对应的网络掩码，在 network address 字段中指定网络地址。当网络掩码全部由二进制的“1”构成时，网络地址就成为了主机地址。

例如，在一个专有网络 192.168.1.0/24 **上，要想使** NIS **正常工作，文件**/var/yp/securenets **应类似于：**

255.255.255.255 127.0.0.1

255.255.255.0 192.168.1.0

为了与该目标保持一致，文件/var/yp/Makefile **也将发生变化。启动** ypserv**，并运行** NIS **初始化会话程序。**

ypserv

/use/lib/yp/ypinit –m

要想运行服务器，可：

/etc/rc.d/init.d/ypserv start

/etc/rc.d/init.d/yppasswd start

要想在下一次重新引导系统时运行服务器，可使用命令 chkkconfig **或通过** serviceboard **开启该服务器。**

chkconfig --add ypserv

chkconfig --add yppasswd

6.5 客户端设置

在文件/etc/passwd **的末尾添加如下条目：**

+::::::

在文件/etc/group **的末尾添加如下条目：**

+:::

启动 ypbind**：**

/etc/rc.d/init.d/ypbind start

要想在下一次重新引导系统时运行 ypbind**，可使用命令** chkkconfig **或通过** serviceboard **开启** ypbind**。**

chkconfig --add ypbind

使用下述命令，验证 NIS **是否正在正常运行：**

ypwhich

nissvr.turbolinux.gr.cn <-- The NIS server name is displayed.

ypcat passwd

user1:ylkXjOSM2R5rQ:501:501::/home/usr1:/bin/bash

user2:aqFAzdBEx8iZE:502:502::/home/user2:/bin/bash

如何通过 ypbinf 指定服务器

编辑文件/etc/yp.conf**，如果文件中没有下行内容，添加它：**

domain [domain name] server [server name]

如何将一个新用户添加到 NIS 服务器

按下述方式使用命令 useradd**，可将新用户添加到** NIS **服务器上。**

useradd [user name]

要想更新 NIS **数据库，可运行：**

/usr/lib/yp/ypinit –m

第七章　其它服务

Turbolinux 7 Server 除了它的各种 Internet 和 Intranet 服务器提供的服务外,还包括一些其他重要的服务。本章将详细介绍每个服务

• SSH (安全外壳)—提供了安全登录到远程主机的方法

• DHCP (动态主机配置协议)—给客户端分配动态 IP 地址

• LDAP (轻型目录访问协议)—在 intranet 和 extranet 上存取网络和用户信息，如用户姓名，Email 地址，电话号码等等

• quota（配额）—通过指定个人用户以及组可使用的数据块和信息节点数，来限制磁盘使用

• IP 伪装–将私有 IP 地址转换为全球 IP 地址

7.1 加密远程登录 SSH

SSH (安全外壳程序) 协议向远程登录提供了更安全的方法。以前在开始登录时，是用 rsh, telnet 等类似的程序，通过网络公开发送用户 ID 和密码。无论是在 intranet 还是 Internet 上，都总是可能出现非法拦截或更改。但是在 SSH 下，所有的通信都被加密，所以，有可能实现更安全的操作。在 Turbolinux 7 Server 中，使用的是开放资源 OpenSSH。因此，从现在开始，ssh 代表 OpenSSH。

OpenSSH 公共站点为：*http://www.openssh.com* all communications are

7.1.1 开始和终止 ssh

启动位于文件/etc/rc.d/init.d/sshd 中的 **ssh** 脚本。

它的选项为：**start**（启动），**stop**（终止），**restart**（重新启动）以及 **status**（状态）

无论何时更改 **ssh** 配置，都必须重新启动 **ssh**，才能使更改生效。

启动 ssh，运行以下命令：

\# **/etc/rc.d/init.d/sshd start**

终止 ssh，运行以下命令：

\# **/etc/rc.d/init.d/sshd stop**

重新启动 ssh，运行以下命令：

\# **/etc/rc.d/init.d/sshd restart**

查看 ssh 的当前状态，运行以下命令：

\# **/etc/rc.d/init.d/sshd status**

用以下命令也能够查看 ssh 是否在运行：

\# **ps aux | grep sshd**

```
root 232 0.0 0.1 2160 68 Z? S May06 0:00 .usr/sbin/sshd
```

如果运行了该命令后，没有出现以上所显示的系统响应，说明 ssh 可能没有运行，或没有被安装。此时，将不得不重新启动 ssh，或者安装后再启动。

使用 serviceboard 也能进行这些操作。.

7.1.2 服务器配置

要想使用 SSH, **服务器上必须运行 sshd 端口监控程序。**Turbolinux 7 Server **通常在引导时启动 sshd，但是要使用前一节介绍的命令查看一下，以确信 sshd 是在运行的。sshd 使用 xinetd 访问控制库。在默认状态下，**Turbolinux 7 Server **不接受外部客户端的请求。所以必须通过编辑访问控制文件***/etc/hosts.allow* and */etc/hosts.deny*，**指定访问。详情请参阅访问控制部分。此外，***/etc/ssh/sshd_config* **也控制这** ssh **的连接。请参阅 sshd 的** man page。

默认禁止 root **用户的远程登录。**

7.1.3 连接方法

访问 SSH **主机，运行：**

$ **ssh** *username***e**@*hostname*

例如，用户"jon"**访问主机** "turbossh"**，运行；**

$ **ssh jon@turbossh**

正确输入密码后登录就完成了。

7.2 动态地址分配 DHCP

对网络上的计算机，要想适用网络资源，就要配置其网络设置，如 IP 地址、网络掩码、网关等。DHCP(动态主机配置协议) 能够用于动态分配地址分配。极大简化了多个客户端的配置和管理，方便了网络的使用和控制。例如，DHCP 特别适合笔记本电脑在不同的网络间频繁地移动，它们的设置必须随每个新的网络环境而变化。

DHCP 服务建立在客户端和服务器之间。客户端向服务器广播请求包括网络地址的网络参数。作为响应，服务器向客户端返回这些参数。然后客户端将这些参数分配给自己使用。

Turbolinux 7 Server 使用 ISC（Internet 软件联盟）DHCP 服务器 Version 2（**dhcp**d）。以下介绍如何创建 DHCP 服务器。

Client Configuration（客户端配置）部分介绍将 Turbolinux 作为 DHCP 客户端运行的方法。客户端不依赖于平台。它能够在 Linux, Windows, Macintosh，或其他操作系统上运行。

7.2.1 DHCP 配置

DHCP 服务器的核心是 **dhcpd** 端口监控程序。通过编辑*/etc/dhcpd.conf* 可以对 **dhcpd** 进行编辑。

在本章的以后部分，将 DHCP 服务器和 DHCP 客户端分别简称为服务器和客户端。

dhcpd.conf 脚本的设置如下：

- 没有被括号括起来的参数是全程应用的
- 括号表示参数应用范围
- 每个参数以分号（;）结尾

以下为典型的 dhcpd.conf 脚本：

```
(1)| option domain-name "fugue.com";
(2)| option domain-name-servers toccata.fugue.com;
|
(3) | option subnet-mask 255.255.255.224;
(4) | default-lease-time 600;
(5) | max-lease-time 7200;
|
(6) | subnet 204.254.239.0 netmask 255.255.255.224 {
(7) | range 204.254.239.10 204.254.239.20;
(8) | option broadcast-address 204.254.239.31;
(9) | option routers prelude.fuge.com;
|}
```

```
|
| subnet 192.5.5.0 netmask 255.255.255.224 {
| range 192.5.5.26 192.5.5.30;
(11)| option domain-name-servers bb.home.vix.com,
gw.home.vix.com;
(12)| option domain-name "vix.com" ;
| option routers 192.5.5.1 ;
(13)| option subnet-mask 255.255.255.224;
(14)| option broadcast-address 192.5.5.31;
(15)| default-lease-time 600;
(16)| max-lease-time 7200;
|}
|
|
 (17)| host passacaglia {
(18)| hardware ethernet 0:0:c0:5d:bd:95;
(19)| filename "vulnix.passacagiliacom";
(20)| server-name "toccata.fugue.com";
|}
|
| host fantasia {
| hardware ethernet 08:00:07:26:c0:a5;
(21)| fixed-address fantasia.fugue.com;
| pp}
|
| host confusia {
| hardware ethernet 02:03:04:05:06:07;
(22)| fixed-address confusia-l.fugue.com, confusia
confusia-2.fugue.com;
| filename "vmunix.confusia";
| server-name "toccata.fugue.com" ;
|}
|
| host confusia {
| hardware ethernet 02:03:04:05:06:07;
| fixed-address confusia-3.fugue.com;
| filename "vmunix.confusia";
| server-name "snarg.fugue.com";
```

```
|}
|
| host confusia {
| hardware ethernet 02:03:04:05:06:07;
| filename "vmunix.confusia";
| server-name "bb.home.vix.com";
|}
```

下面解释以上所示脚本中的各行：

（1）**指定客户端用于解析主机名称的域名。对应于**/etc/resolv.conf **中的搜索行**

（2）**指定域名服务器。如果不止一个，用逗号分开。能够用** IP **地址指定域名服务器，但是如果** DHCP **服务器能够解析域名服务器的主机名称，那么就不必用** IP **地址指定域名服务器。**

（3）**指定客户端将要使用的子网掩码**

（4）**指定服务器分配给客户端的** IP **地址的有效时限（单位为秒）。在时限结束之前，当客户端运行时，它能够使用相同的** IP **地址。由于客户端再一次请求服务器提供相同的** IP **地址，在时限结束以前，在客户端运行的整个期间，能够继续使用相同的** IP **地址。如果客户端没有请求，在租借期内，服务器继续维持租借给客户端的** IP **地址。租期满后，**IP **地址能够被分配另一个客户端。**

（5）**这是当客户端请求指定期限的租期时，服务器能够允许的最长租期（单位为秒）。如果客户端没有指定租期，就使用默认租期。**

（6）**确定了参数应用的界限。括在花括号中的参数就是一个示例，该参数将应用于属于子网** 204.254.239.0 **的客户端。属于服务器的所有子网的配置应该被申明，即使有一些并没有获得** DHCP **服务。**

(7)…,(10)...

指定租借的 IP **地址的范围。**IP **地址必须包括在子网内。如果在指定范围内的地址可以被动态分配给** BOOTP **客户端，可以指定** *dynamic-bootp* **标志位。**

（8）**指定客户端将要使用的广播地址**

（9）**指定路由器。如果不止一个，用逗号分开。**

(11)…-(16)...

重新写包含在子网 192.5.5.0 **中的客户端的全程定义的参数的定义**

（17）**定义使用花括号中包含的参数的主机（客户端）**

（18）**指定客户端机器的网卡** MAC **地址（唯一分配给每个个人网卡）。要想查看** MAC

地址，运行：

ifconfig | grep eth0

(19) **指定客户端机器需要从服务器加载引导文件时的初始引导文件名。通常指定内核图像文件**

(20) **指定客户端机器需要从服务器加载引导文件时的 bootpd 服务器名称**

(21)…,(22)...

指定将要分配给指定主机的 IP 地址和主机名。当指定主机名时，服务器必须解析主机名。当指定范围时，客户端地址从那个指定的范围中选择，如以下例子所示。

以下为 *dhcpd.conf* **的简单例子：**

```
option domain-name "mydomain";
option domain-name-servers 192.168.1.2;
subnet 192.168.1.0 netmask 255.255.255.0 {
range 192.168.1.244 192.168.1.254;
option routers 192.168.1.1;
}

subnet 192.168.2.0 netmask 255.255.255.0 {
}
```

这个例子指定将不向子网 192.168.2.0 提供 DHCP 服务，因为它不在指定的范围内。

7.2.2 启动和终止

DHCP **启动脚本位于** int /etc/rc.d/init.d/dhcpd。

启动脚本选项为： start（启动），stop（终止），restart（重新启动）以及 status（状态）。

无论何时更改 DHCP 配置，都必须重新启动 DHCP，才能使更改生效。

启动 DHCP，运行以下命令：

/etc/rc.d/init.d/dhcpd start

中止 DHCP，运行以下命令：

/etc/rc.d/init.d/dhcpd stop

重新启动 DHCP，运行以下命令：

/etc/rc.d/init.d/dhcpd restart

查看 DHCP 的当前状态，运行以下命令：

/etc/rc.d/init.d/dhcpd status

用 ps 命令，也能够查看是否 DHCP 正在运行：

ps aux | grep dhcpd

root 766 0.2 0.2 1764 732 ? S 08:13 0:00 dhcpdd

如果运行了该命令后，没有出现以上所显示的系统响应，说明 DHCP **没有运行，或没有被安装。此时，必须重新启动** DHCP**，或者安装后再启动。**

如果需要在每次系统重新启动时，启动 dhcpd ，运行：

chkconfig --add dhcpd

如果需要在每次系统重新启动时，不启动 dhcpd ，运行：

chkconfig --del dhcpd

使用 serviceboard 也能够启动和终止 dhcpd，并查看其状态。

7.2.3 当 DHCPD 不正常运行时

当 dhcpd 不正常运行时，设法在前台以调试模式运行它。运行：

dhcpd -d –f

终止 dhcpd**，按** Ctrl-C.

如果因为客户端正在运行 Windows95/98/NT**，dhcpd 不正常运行，在启动 dhcpd 之前，改变路由表。运行：**

route add -host 255.255.255.255 eth0

7.2.4 DHCP 软件包

Turbolinux 7 Server **包括以下软件包：**

DHCP **服务器** dhcp **软件包**

DHCP **客户端** dhcp-client **软件包**

用 rpm 命令能够查看各种软件包中的文件：

rpm -ql dhcp

rpm -ql dhcp-client

dhcpd **使用以下文件：**

/etc/rc.d/init.d/dhcpd	**dhcpd 启动脚本**
/usr/sbin/dhcpd	DHCP **服务器程序**
/var/dhcp/dhcpd.leases	DHCP **客户端租用数据库**

7.2.5 客户端配置 (Turbolinux)

遵照以下步骤，将 *Turbolinux* **作为** DHCP **客户端运行：**

1. 运行 netcfg:

netcfg

2. 从 Network Interface（网络接口中）中选择 DHCP 将使用的接口。如果所列出来的当中没有你所需要的，就选择 Add，创建一个。

3. 选择 Edit，查看 [Use DHCP]。不必输入 IP 地址、网络掩码、网络地址、以及广播地址，输入所有其他的剩余设置，然后退出 netcfg。

4. 重新启动网络，运行 DHCP：

/etc/rc.d/init.d/network restart

7.3 轻量级目录访问协议 LDAP

计算机网络经过长期的发展，不同的操作系统和应用程序以不同的格式在网络上存储了大 量的信息，一个网络管理员无法在一个集中的信息库中，以方便的方法管理网络信息和资源。用户必须使用不同的应用程序获取不同的信息和资源，这大大增加了用户的负担，也使许多信息难于共享，从而在一定程度上制约了网络的发展，因而需要一种新的技术，能够以通用的格式和方式实现信息的存储和共享，实现网络的共享。目录服务应运而生, 目录服务将分散在网络各处的资源和信息汇集在一起，从而有可能有效地管理他们。LDAP （轻型目录访问协议）是主干协议 X.500 DAP (目录访问协议)的替代物。LDAP 是为 Internet 的使用而设计的，比 DAP 小，使用简单。

LDAP 目录服务是开放，灵活和高速协议，它能在内部网和外部网上存取网络和用户信息，诸如用户名，email 地址，电话号码，等等。

简单地说，目录在网络系统中是指网络资源的清单，它以一定的格式记录了现实世界中大量的信息，供用户（人、计算机应用程序等）做各种查询和修改。目录服务是指网络系统将网络中的各种资源信息集中管理起来，为用户提供一个统一的清单。目录服务在某种程度上讲它就是代表网络用户及资源的基于对象的数据库。每个对象中都存储着与特定用户和网络资源有关的信息。对象可以在目录的树状结构中分层存储。便于用户建立一个与企业组织结构一致的网络结构。网络上的每个用户及资源均与别的用户和资源有关联，目录能够通过鉴定和授权来管理和控制人和计算机、计算机和计算机之间的关系。用户被鉴定意味着用户与网络组件两者能互相识别，因此能防止他人侵入系统偷取信息。用户被鉴定后，网络即授权该用户管理或使用他有权管理和使用的网络资源。用户的权限可以是全局的、组 织内的或跨工作组的，网络管理员可以为特定的用户赋予特殊的权限，以满足那些处于目录树各个层次中的个别用户对网络资源的特殊需要。

如果需要开发一种提供公共信息查询的系统，如通过用户姓名能够获得该用户的邮件地址、家庭住址等信息，如 Yahoo 提供的 People search 服务。一般的设计方法可能是采用基于 WEB 的数据库设计方式，即前端使用浏览器而后端使用 WEB 服务器加上关系数据库。Linux 系统的典型实现可能是 Linux + Apache + Mysql，Apache 和数据库之间通过 PHP3 提供的函数进行连接。使用上述方法的缺点是后端关系数据库的引入导致系统整体的性能降低和系统的管理比较繁琐，因为需要不断的进行数据类型的验证和事务的完整性的确认；并且前端用户对数据的控制不够灵活，用户权限的设置一般只能是设置在表一级而不是设置在记录一级。

目录服务的推出主要是解决上述数据库中存在的问题。目录与关系数据库相似，是指具有描述性的基于属性的记录集合，但它的数据类型主要是字符型，为了检索的需要添加了 BIN（二进制数据）、CIS（忽略大小写）、CES（大小写敏感）、TEL（电话型）等语法（Syntax），而不是关系数据库提供的整数、浮点数、日期、货币等类型，同样也不提供象关系数据库中普遍包含的大量的函数，它主要面向数据的查询服务（查询和修改操作比一般是大于 10:1），不提供事务的回滚（rollback）机制，它的数据修改使用简单的锁定机制实现，它的目标是快速响应和大容量查询并且提供多目录服务器的信息复制功能。

LDAP（Lightweight Directory Acess Protocol）是目录服务在 TCP/IP 上的实现（RFC 1777 V2 版和 RFC 2251 V3 版）。它是对 X500 的目录协议的移植，简化了实现方法，所以称为轻量级的目录服务。在 LDAP 中目录是按照树型结构组织，目录由条目（Entry）组成，条目相当于关系数据库中表的记录；条目是具有区别名 DN（Distinguished Name）的属性（Attribute）集合，DN 相当于关系数据库表中的关键字（Primary Key）；属性由类型（Type）和多个值（Values）组成，相当于关系数据库中的域（Field）由域名和数据类型组成，只是为了方便检索的需要，LDAP 中的 Type 可以有多个 Value，而不是关系数据库中为降低数据的冗余性要求实现的各个域必须是不相关的。LDAP 中条目的组织一般按照地理位置和组织关系进行组织，非常的直观。LDAP 把数据存放在文件中，为提高效率可以使用基于索引的文件数据库，而不是关系数据库。LDAP 协议集还规定了 DN 的命名方法、存取控制方法、搜索格式、复制方法、URL 格式、开发接口等。

Linux 支持的 LDAP 服务器一般有 Michigan 大学开发的免费软件包和 Openldap 组织基于 Michigan 大学的开发包提供的 Openldap 免费软件发行包，其中 Openldap 发行包安装配置更加简单。

本节介绍一个简单的示例：Netscape 邮件客户端使用 LDAP 服务器作为地址簿，和使用开放资源 OpenLDAP 作为使用 LDAP 的应用服务器。

OpenLDAP 公共站点 *http://www.openldap.org/.*

7.3.1 创建 LDAP 服务器数据库

OpenLDAP 服务器在 */usr/tmp* 目录中创建数据库。但是如果数据库比较大，建议创建在空间更宽敞的地方，如*/home*。

为 LDBM 文件创建一个区域，LDBM 包含二进制索引以及 LDAP 使用的文件：

```
# cd /home
# mkdir -p ldap/ldbm/abook/public
```

注意：

能够创建使用 */etc/passwd* 作为数据库的 SLAPD (独立轻型访问协议) 服务器；或者类似 HTTP 的 CGI (公共网关接口)的 SLAPD 服务器，HTTP 的 CGI 是调用交互程序。但是通常使用 LDBM 系统。

7.3.2 创建 slapd.conf 文件

slapd.conf 文件创建在 /etc/ldap 目录下。设置许可为 600，超级用户(root)所有权。如果

您的要使用该配置文件作为您试验用的例子请保存好原有的文件.

对这个配置文件的关键修改是对 suffix 后缀为本地的组织形式，可以按照域名的形式，也可以按照组织模式。其中的 rootdn 定义了本地目录树的根，rootpw 即是相对于本目录树的管理员口令，缺省是使用的明文为"secret"。其中的 replica 指定备份目录服务器的地址，如果是备份服务器则不需要 replica 配置项，而是添加 udpatedn=主目录服务器的地址，同时指定 referral 为主目录服务器。同时，缺省的目录数据是以 ldbm 形式（Linux 中实际 gdbm 格式）存放在/usr/tmp 目录中。Access 定义了对目录信息的访问信息，它是基于条目的，即用户自己可以通过输入自己的口令修改自己的数据，其口令存放在自己的口令域（userpassword）中。.

本示例文件内容(系统安装完成后的默认文件):

```
# /etc/ldap/slapd.conf
# $OpenLDAP: pkg/ldap/servers/slapd/slapd.conf,v 1.8.8.6 2001/04/20 23:32:43 kurt Exp $
#
# See slapd.conf(5) for details on configuration options.
# This file should NOT be world readable.
#
include             /etc/ldap/schema/core.schema

# Define global ACLs to disable default read access.

# Do not enable referrals until AFTER you have a working directory
# service AND an understanding of referrals.
#referral           ldap://root.openldap.org

pidfile             /var/lib/slapd.pid
argsfile            /var/lib/slapd.args

# Load dynamic backend modules:
#  modulepath       /usr/sbin/ldap
#  moduleload       back_ldap.la
#  moduleload       back_ldbm.la
#  moduleload       back_passwd.la
# moduleload        back_shell.la

#######################################################################
# ldbm database definitions
#######################################################################

database            ldbm
suffix              "dc=my-domain,dc=com"
#suffix             "o=My  Organization  Name,c=US"
rootdn              "cn=Manager,dc=my-domain,dc=com"
#rootdn             "cn=Manager,o=My  Organization  Name,c=US"
```

```
# Cleartext passwords, especially for the rootdn, should
# be avoid.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw                    secret
# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd/tools. Mode 700 recommended.
directory              /var/lib/openldap-ldbm
# Indices to maintain
index      objectClass          eq
```

注意：以上示例没有谈及安全问题。如果你能全程访问 LDAP 服务器，你必须注意地址簿的内容。

建议修改 access **，仅仅授予** LAN **内的用户以及特殊用户许可，通过** LDAP **协议修改或删除条目。**

更改 rootpw **文件。利用** rootdn, **用** LDAP **协议,能够在** LDBM **中添加，删除或修改条目。**

注意：几乎所有的都被编入索引了。包含破折号(-)的数字字段或电话号码中的空格都被保存。属性 *userpassword* 和 d *labeleduri* 的值都是区分大小写的。以上文件中的属性由 Netscape Communicator 和 Microsoft 地址簿来识别。应用程序不支持的属性一般被忽略。

7.4 启动 LDAP 服务器

LDAP **服务的启动脚本为** */etc/rc.d/init.d/lda*p。**要启动** LDAP **服务器，以超级用户身份运行以下命令：**

/etc/rc.d/init.d/ldap start

以上命令的运行是假设数据库已经被正确配置。*slapd.conf* **也已经正确设置。要想查看** LDAP **服务器是否正在适当运行，运行：**

/etc/rc.d/init.d/ldap status

也可以使用 serviceboard 启动、终止和查看 ldap 状态。

7.4.1 测试服务器

对大多数用户，运行：

```
# ldapsearch -x -b ‘’ -s base ‘(objectclass=*)’ namingContexts
version: 2

#
# filter: (objectclass=*)
# requesting: namingContexts
#
```

```
#
dn:
namingContexts: dc=my-domain,dc=com

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

这是这是正确的结果,**如果不同**,**请仔细检查**.

7.4.2 LDBM 数据库的转换

因为 LDAP **服务器不能处理** LDIF **文本文件，**LDIF **文件必须被转换为二进制索引。您可以使用 ldif2ldbm 或 ldapadd 命令**.

这是 LDIF **文本文件的例子**, **假设该文件名称为** example.ldif:

注意,文件中不能有多余的空格,否则试验可能失败!

```
dn: dc=my-domain,dc=com
objectclass: dcObject
objectclass: organization
o: Example Company
dc: my-domain

dn: cn=Manager,dc=my-domain,dc=com
objectclass: organizationalRole
cn: Manager
```

转换该文件为数据库格式:

```
# ldif2ldbm -i example.ldif
```

ldif2ldbm 假设 *[/etc/ldap/spald.conf]* **存在**,**同时** LDAP **没有运行**,**该命令不能在** LDAP **运行时使用**.

如果您需要 LDAP **运行时增加数据项请使用如下命令**:

```
# ldapadd -v -x -D "cn=Manager,dc=my-domain,dc=com" -w secret -f example.ldif
ldap_initialize( <DEFAULT> )
add objectclass:
        dcObject
        organization
add o:
        Example  Company
add dc:
```

```
                my-domain
adding new entry "dc=my-domain,dc=com"
modify complete

add objectclass:
                organizationalRole
add cn:
                Manager
adding new entry "cn=Manager,dc=my-domain,dc=com"
```

7.4.3 检查 LDAP 工作状况

运行命令及显示结果:

```
# ldapsearch -x -b 'dc=my-domain,dc=com' '(objectclass=*)'
version: 2

#
# filter: (objectclass=*)
# requesting: ALL
#

# my-domain, com
dn: dc=my-domain,dc=com
objectClass: dcObject
objectClass: organization
o: Example Company
dc: my-domain

# Manager, my-domain, com
dn: cn=Manager,dc=my-domain,dc=com
objectClass: organizationalRole
cn: Manager

# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 2
```

这说明我们的数据已经进入LDAP**数据库并且**LDAP**运行正常**.

7.4.4 LDAP 的其他问题

以下部分讨论有关LDAP需要注意的一些其他问题。

在数据库中保存多语言数据

有时地址中可能即有英文字符，又有其他语言的字符。在这种情况下，使用下一个类型。

无论何种语言，必须将 *lang* 设置为适当的语言缩写代码。例如，对中文繁体字，*lang = zh_TW* ；中文简化字，*lang= zh_C*N。LDAP 数据库中的所有字符串必须使用 UTF-8 编码中的统一字符编码标准。例如，如果保存以 EUC-JP 编码的数据，诸如 Netscape 等应用程序可能会扰乱它们。

对同一属性，能够有多个值。在一个 LDIF 条目中添加多个 email 地址时，应该是一行一个 email 地址：

```
mail: dr.feelgood@powers.com
mail: mini.me@powers.com
```

保存二进制数据

以 Base64 格式表示的数据在 LDIF 文件中保存为二进制数据。

能够将很长的行分为几个短行。.

以下是一个*/usr/sbin/ldi*f 的 Base-64 LDIF 条目的示例：

```
# /usr/sbin/ldif -b jpegPhoto < picture.jpeg > picture.ldif
# /usr/sbin/ldif -b audio < hello.au > audio.ldif
# /usr/sbin/ldif -b "usersmimecertificate;binary" < cert.p12 >
cert.ldif
```

使用 "referral"

如果当前的 LDAP 服务器没有想要的条目,能够在 lapd.conf 中使用 referral 设置,LDAP 服务器将给客户端一个 fallback。

反射 LDAP 服务器

OpenLDAP 包含 **slurp**d, 它是端口监控程序，将对主 **slapd** 数据库的更改发布给 **slapd** 复制件。

7.5 磁盘配额(quota)

利用 quota **（磁盘配额），能够通过指定数据块数和信息节点数，限制用户以或组的磁盘占用。一个数据块的默认值为** 1KB**。如果磁盘使用的限制为** 10MB**，**1MB = 1024KB**，则向用户提供的总数据块数为** 1024**。**UNIX **文件系统创建文件时，有关文件的信息，如许可等存储在名为** *inode* **的区域。当初格式化文件系统时，已经决定了可能的信息节点数。即使有剩余的磁盘空间，一旦用完了所有的信息节点，那些剩余的磁盘空间也就不能再使用了。因为小文件仅要求使用一个信息节点，所以节点数和文件数大致相同。**

使用 dumpe2fs **命令查看信息节点数。**

当文件系统是 *ext2***（标准** Linux**）文件系统格式**, **要想查看***/dev/hda1* **上能够使用的信息节点数，输入：**

```
# dumpe2fs /dev/hdal | grep 'Inode count:'
```

要想查看在*/dev/hda*l **目录上的，***ext2* **格式化的文件系统上剩余的空闲信息节点数，输入：**

```
# dumpe2fs /dev/hdal | grep 'Free inodes:'
```

/etc/fstab

在*/etc/fsta*b **中添加参数，开启文件系统的配额设置。对于用户，添加** *usrquota* **；对于组，添加** *grpquota* **。**

按照以下所示模式，改写*/etc/fstab***：**

对于*/home* **文件系统中的用户磁盘配额，使用：**

```
/dev/hda2 /home ext2 defaults,usrquota 1 1
```

对于*/home* **文件系统中的组磁盘配额，使用：**

```
/dev/hda2 /home ext2 defaults,grpquota 1 1
```

对于*/home* **文件系统中的用户磁盘配额和组磁盘配额，使用：**

```
/dev/hda2 /home ext2 defaults,usrquota,grpquota 1 1
```

修改完成后需要重新启动以使更改后的 */etc/fstab* **设置生效。如果不希望重新启动而使用磁盘配额功能可以运行类似于以下的命令：**

```
mount -o usrquota /dev/dha2 /home
```

当然，/dev/hda2 **没有被当前的文件系统使用**,**而且是一个已经格式化好的分区**.

如果 */etc/fsta*b **中已经有上述的这些参数，加载文件系统就简单多了：**

```
mount /home
```

生成 quota 文件

配置文件位于 quota 开启的文件的根目录。文件用以下名称保存：

用户配额 quota.user

组配额　 quota.group

与大多数的配置文件不同，磁盘配额(quota)配置文件不能直接编辑。必须使用 edquota 命令进行编辑

编辑器配置

edquota 的默认编辑器是 vi。如果想使用其他的编辑器，需要将环境变量 EDITOR 设置为想要的编辑器，然后再运行 edquota。

例如，要想使用 Xemacs 作为 quota 的默认编辑器，命令如下：

```
# export EDITOR=xemacs
# edquota -u username
```

利用 edquota 进行配置

当第一次运行 edquota 时，配置文件并不自动创建。请按如下命令创建,以后再次运行磁盘配额设置不要再运行这些命令,否则原有的设置将被清除.

假设在 */home* 文件系统中设置用户/组磁盘配额，运行命令如下：

```
# touch /home/quota.user <-- 生成文件 quota.user
# chmod 600 /home/quota.user <-- 除了超级用户(root)外，禁止所有其他用户的读写操作
# touch /home/quota.group
# chmod 600 /home/ quota.group
# /sbin/quotacheck –avug        ←---初始化某些设置,如果不进行可能会出错
```

然后，磁盘配额设置命令如下所示(假设用户 scott 已经存在,组 support 也已经存在)：

```
# edquota -u scott <-- 为用户"scott"设置配额
# edquota -g support <-- 为组 "support"设置配额
```

在与 quota 有关的命令中，使用-u 选项设置用户 quota；使用-g 选项设置组 quota。如果两个选项都不指定，就假设请求用户 quota。

例如，要想设置用户"scott"的 quota，运行：

```
# edquota -u scott
```

修改用户 scott 的配额如下:

```
Disk quotas for user scott (uid 501):
  Filesystem       blocks      soft      hard     inodes     soft     hard
  /dev/sda7           104       900      1200         28     9000    12000
```

blocks 列限制数据块的数目；inodes 列限制信息节点数，前面的 soft/hard 是对块的限制;后面的 soft/hard 是对文件的限制.

hard limit（硬限制）	用户不能超过磁盘使用的硬限制。
soft limit（软限制）	达到软限制时，警告用户，并给用户一个宽限期。在这个期限内，用户能够在磁盘上进行写操作，直至达到硬限制。但是一旦宽限期结束，即使还没有达到硬限制，用户也不能再向

磁盘中写了。如果设置为 0 表示没有时间期限。

要想设置宽限期，运行：

edquota -u -t <-- 用户配额

block grace period: 表示数据块数的宽限期

inode grace period: 表示信息节点数的宽限期。宽限期用天，小时，分钟或秒表示。

时间单位可以是：天，小时，分钟或秒。

强制实施软限制之前的用户宽限期：

/dev/hda5: block grace period: 1 days, file grace period: 24 hours

以上的例子表示，如果用户‘scott’使用的数据块超过了 9000 个（信息节点数为 900），24 小时以后，他将不能访问磁盘。当使用的数据块超过了 12000 个（信息节点数为 1000），他将不能访问磁盘。

如果要为 100 个用户设置配额，为每一个用户都运行一遍 **edquota -u** 会花费很多时间。如果每个用户的设置都相同，可以复制。所以，如果用户 derik, john, 和 scott 有相同的设置，可以运行：

edquota -p scott derik john

注意,顺序不能出错!

开启 quota

当启动系统时，quota 被默认开启。如果需要手动开启，可以使用 quotaon 命令：

quotaon –avug

关闭，运行：

quotaoff –avug

quota 的其他命令

repquota 报告*/etc/fstab* 中设置有配额的所有文件系统的状态.

quotacheck 扫描文件系统的磁盘使用情况，并输出到 *quota.use*r

quota 显示指定用户和组的磁盘使用情况和限制。普通用户能够运行这个命令

其他命令请参见 quota 在线 的 man page: man quota

7.6 IP 伪装

IP 伪装功能是将本地 IP 地址转换为外部网络 IP 地址从而允许多台计算机通过一台主机一个 IP 地址访问外部网络。Turbolinux 7 Server 使用 iptables 程序实现这个转换(原来使用 ipchains)。

iptables 用于 Linux 2.4.x 内核控制网络防火墙的匹配规则（信息包过滤）。这是以往的 ipfwadm 提供的功能的扩展集。

iptables 能够控制其他主机对本机的访问,例如我们要禁止 test.turbolinux.gr.cn 对本机的访问可以用如下命令:

iptables -A INPUT -s test.turbolinux.gr.cn -j REJECT

这样,来自主机 test.turbolinus.gr.jp 的所有访问都将被阻止。对于 test.turbolinux.gr.cn 而言,就好像网络上根本不存在我们正在使用的这台主机一样。这些选项的意思是将规则"无论何时，只要有来自主机 test.turbolinus.gr.jp 的访问企图就转到目标 REJECT"添加到输入链。

运行以下命令，可以列出当前链的状态。刚才添加的条目将会出现。

iptables -L INPUT

在继续下一步之前，删除到目前为止所做的所有设置。使用-D 选项从 IP 链中删除一个或多个规则：

iptables -D INPUT 1

使用-F 选项，可以同时全部删除规则：

iptables -F INPUT

有可能进行更细致的配置。例如，仅仅堵塞你自己主机上的 telnet port，使其不能从指定的域连接，可以运行类似于以下的命令：

iptables -A INPUT -p TCP --source-port telnet -s turbolinux.gr.cn/25 -d test2.turbolinux.gr.cn -j REJECT

这个命令阻断 telnet port 上从域 tubolinux.gr.jp/25 到 test2.turbolinux.gr.cn 的连接。

如果想要阻断指定主机的访问，可以应用以上设置；反过来 ，如果只想允许指定主机的访问，也能够进行设置。该命令如下：

iptables -A INPUT -p TCP --source-port telnet -s test.pht.com.cn -d test2.turbolinux.gr.cn -j ACCEPT

iptables -A INPUT -p TCP --source-port telnet -s 0.0.0.0/0 –d test2.turbolinux.gr.cn -j REJECT

以上的命令序列进行以下操作：

- 设置应用给以主机自己为目标的信息包的规则
- 允许使用输出链来配置从主机自己到另一个主机的信息包
- 允许使用正向链来设置信息包路由规则

因为 IP 伪装是一种路由，要使用和配置正向链和 MASQ 目标。在配置路由时，运行以下所示命令。注意，路由是默认关闭的，需要确保开启路由。

echo 1 > /proc/sys/net/ipv4/ip_forward

iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

如果使用用户自定义的链，动态添加或删除与指定的设备和主机有关的规则组就会更方便。这些规则优于前面介绍的管理 IP 链的方法。要想了解更多的其他选项，请查阅 iptables man page。

7.7 Squid 代理服务器

代理服务是指由一台拥有标准 IP 地址的机器代替若干没有标准 IP 地址（以下称内部地址）的机器和因特网上的其他主机打交道，提供代理服务的这台机器称为代理服务器。拥有内部地址的机器想到因特网上查找资料时，先把这个请求发给拥有标准 IP 地址的代理服务器，由代理服务器把这个请求通过它的标准 IP 地址发到请求的目标地址。然后目标地址的服务器把返回的结果发回给代理服务器，代理服务器再原封不动的把资料发给最初那台拥有内部 IP 地址的机器。这样就完成了一次内部机器访问因特网的一个过程。若干拥有内部地址的机器就组成了内部网，代理服务器的作用就是勾通内部网和因特网，解决内部网访问因特网的问题。而且这种代理是不可逆的，因特网上的主机不能访问任何一台拥有内部地址的机器，这样又可以保障内部资料的安全性。所有这些过程对用户是透明的,用户根部不用管其中的具体细节.

Squid 代理服务器可以设置一个很大的缓存，把常去网站内容存储到缓存中，这样，内部网的机器再访问那些网站，就可以从缓存里调用了。这样可以加快内部网浏览因特网的速度，减少不必要的网络带宽占用。Squid 不仅支持 HTTP 协议，还支持 FTP,GOPHER,SSL 和 WAIS 等协议。

7.7.1 配置方案

squid 主配置文件 /etc/squid/squid.conf

acl deny_ip_01 dst 1.1.1.1

http_access deny deny_ip_01

以上两行是基于 IP 的访问控制

acl deny_url_01 url_regex http://www.www.www

http_access deny deny_url_01

以上两行是基于 URL 的访问控制

http_port 3128 # HTTP 协议代理默认代理端口

cache_mem 32 MB #开劈一块内存区域作为缓冲

cache_dir ufs /home/squid/cache 1024 16 256

开劈硬盘空间，作为缓冲区，这块区域的分布是连续的，逻辑关系由管理员设定

cache_access_log /var/log/squid/access.log

该 log 文件是用来描述每次客户请求 HTTP 内容时，高速缓

存命中或未命中的项目。同时描述提出请求的主机身份及它们所需的内容。

cache_log /var/log/squid/cache.log

＃用于描述当 squid 守护进程启动时，可看到有多少内存、交换空间，

高速缓存目录的位置，所接受的连接类型及接受连接的端口。

cache_store_log /var/log/squid/store.log

＃用于描述页面从高速缓存中被调入调出的情况。

pid_filename /var/run/squid.pid

＃管理员可以通过查看此文件了解当前执行的 squid 进程。

dns_nameservers 192.168.0.1

＃定义域名解析服务器的地址

acl all src 0.0.0.0/0.0.0.0

cache_mgr root@weboa.com.cn

＃设置 cache 管理员的邮件箱地址

reference_age 3 days

＃设置缓冲区的更新周期

maximum_object_size 4096 KB

＃设置允许被缓存的一次性最大请求

squid 的配置文件很复杂，功能强大，我们所作的仅是以需求为导向，配置出符合我们自己需要的服务器就可以了。

7.7.2 Squid 的启动和关闭

启动 Squid:

/etc/rc.d/init.d/squid start

停止 Squid:

/etc/rc.d/init.d/squid stop

您也可以使用 serviceboard 命令,然后选择 squild 进行启动、关闭等操作。

测试方法是在客户机下打开浏览器，按上述设置正确设置代理服务器，然后看是否能够使用浏览器上网。

7.7.3 透明代理(重定向)

最常见的透明代理的使用是结合 iptables **和** Squid**，实现局域网内用户不用设置任何代理服务器就可以透明地使用代理上网。**

假设网卡 eht0、eth1 **已经配置好**,Squid **的** HTTP **端口运行在** 3128**，请使用下面的规则：**

```
# iptables -t nat -A PREROUTING -i eth1 -p tcp -s 10.0.0.0/24 --dport 80 -j DNAT --to 10.0.0.1:3128
```

同时设置/etc/squid/squid.conf **如下：**

```
http_port 3128
httpd_accel_host virtual
httpd_accel_port 80
httpd_accel_with_proxy on
httpd_accel_uses_host_header on
```

第八章　基于 web 的系统管理

8.1　为什么使用 webmin

我们进行计算机系统管理时通常会采用修改配置文件、使用文本介面的配置工具、图形介面的配置工具等方法。

这些方法因不同的计算机或操作系统而不同，或者需要在本机或至少登录到本机才能进行这些管理工作。

进行不同的管理工作需要记住不同的配置文件或配置命令。

Webmin 是基于WWW界面的管理工具，该管理工具能够管理所有的系统配置，支持大多数不同的操作系统，对这些系统的配置方法也很类似，界面风格完全相同。进行配置时可以在本机也可以在其它计算机上，您只要通过浏览器连接到被管理主机的端口上，通过浏览器就能进行系统管理工作了。

Webmin 可以管理 apache、bind、DHCP、FTP、mail、MYSQL、postSQL、SQUID、sendmail、等几乎所有的系统服务，还可以管理 LILO 启动、进行磁盘分区、设置打印机等。同时用户可以根据需要增加新的系统管理功能模块组件，具有很大的灵活性、扩展性。

8.2　webmin 的启动、停止和登录

出于系统安全方面的考虑，系统启动后默认不启动 webmin,如果需要默认启动，请使用 serviceboard 命令或 setup 命令然后选择 “系统服务”进行设置。

启动脚本文件是 /etc/rc.d/init.d/webmin 。

它的选项为：**start**（启动），**stop**（终止），**restart**（重新启动）以及 **status**（状态）

启动 **webmin**，运行以下命令：

```
# /etc/rc.d/init.d/webmin start
```

终止 **webmin**，运行以下命令：

```
# /etc/rc.d/init.d/webmin stop
```

重新启动 **webmin**，运行以下命令：

```
# /etc/rc.d/init.d/webmin restart
```

查看 **webmin** 的当前状态，运行以下命令：

```
# /etc/rc.d/init.d/webmin status
```

用以下命令也能够查看 webmin 是否在运行：

```
# ps auxw | grep miniserv.pl
798 ?          00:00:00 miniserv.pl
```

启动 webmin 后您就可以使用任何支持 https 加密传输的浏览器进行系统管理工作了，默认可以从任何能够连接到这台主机的计算机进行管理工作，如果需要限制管理用户的地址，请使用 webmin 进行调整。

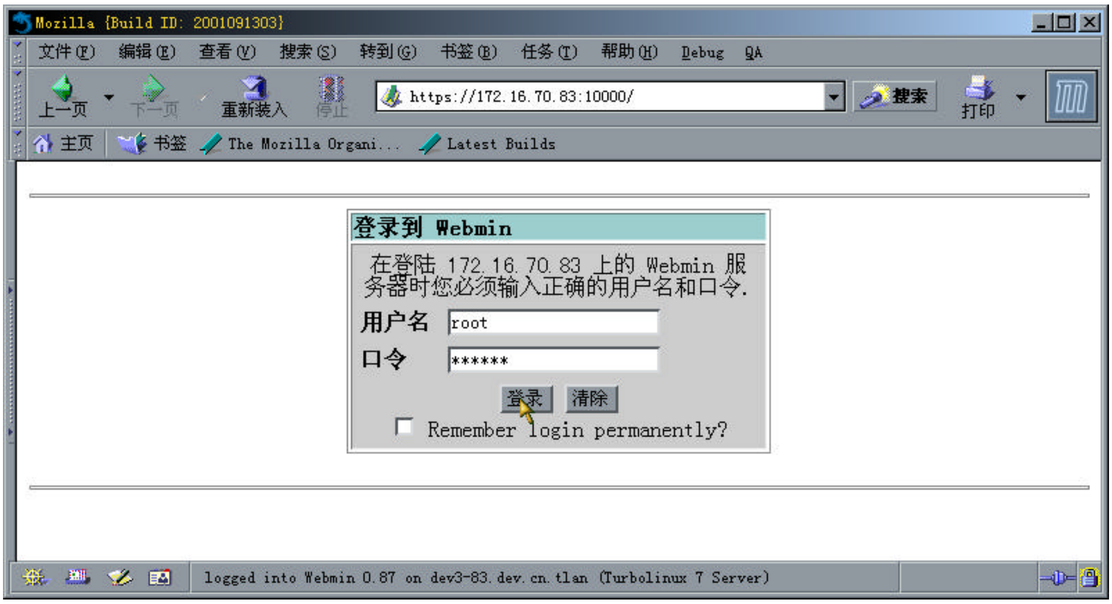
最好在完成系统管理工作后关闭 webmin 防止入侵。

您可以使用 Turbolinux 自带的 mozilla、KDE 浏览器，也可以在其它主机上使用 IE 浏览器。

在浏览器中输入要管理的主机名称或地址，webmin 默认使用的端口号是 10000，例如在本机您可以这样输入地址：https://localhost:10000 ,注意输入的必须是 https，不是默认的 http。

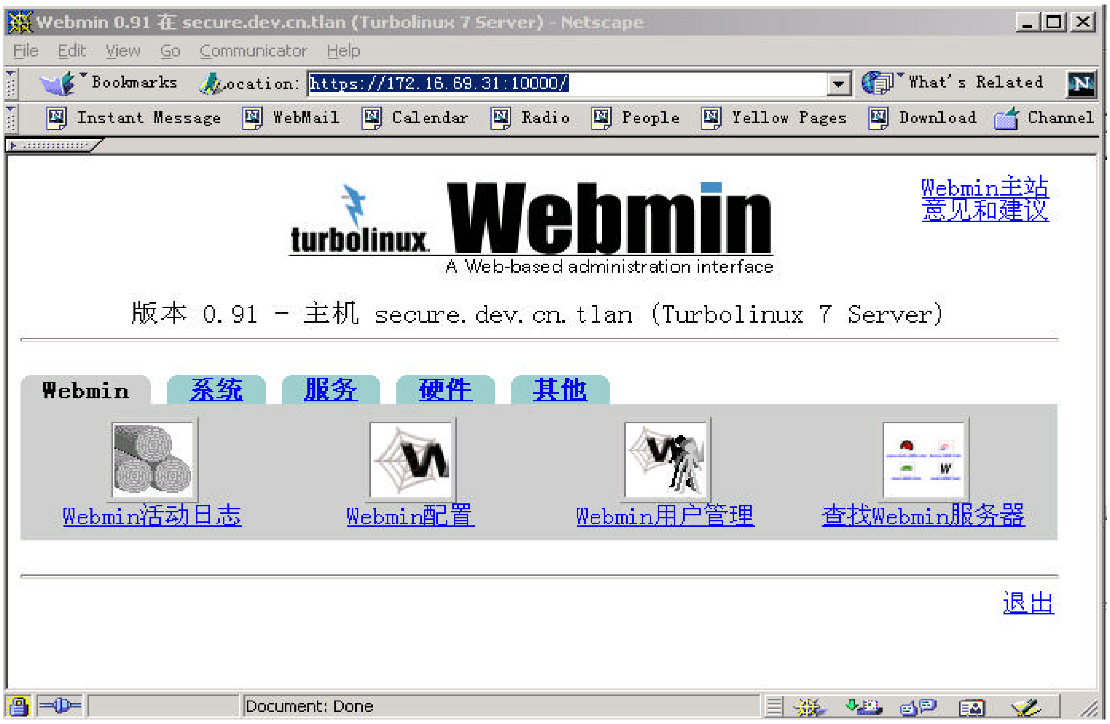
最开始默认的用户名和口令是系统超级帐号 root 的用户名和口令，该帐拥有所有的系统管理的权限。

输入正确的用户名和口令后，用鼠标点击 “ 登录 ”就进入了 webmin 的管理界面。



8.3 webmin 功能概述

webmin 的管理组分为 webmin、系统、服务、硬件、其它几个部分，用鼠标点击对应的书签就可以使用该功能组。



- webmin 用于 webmin 本身的管理，例如使用 webmin 的用户的增加、删除、修改等。
- 系统 用于 turbolinux 系统本身的管理，例如 nfs 共享输出目录、日志、磁盘配额等。
- 服务 用于 turbolinux 系统服务方面的管理例如 ftp、www、sendmail、smb 共享等。
- 硬件 用于 turbolinux 系统和硬件相关方面的管理，例如磁盘分区、世界时间同步等。
- 其它 包括系统服务状态显示、ssh 登录、文件管理、以及用户自己定制的命令等。

8.4 webmin 管理

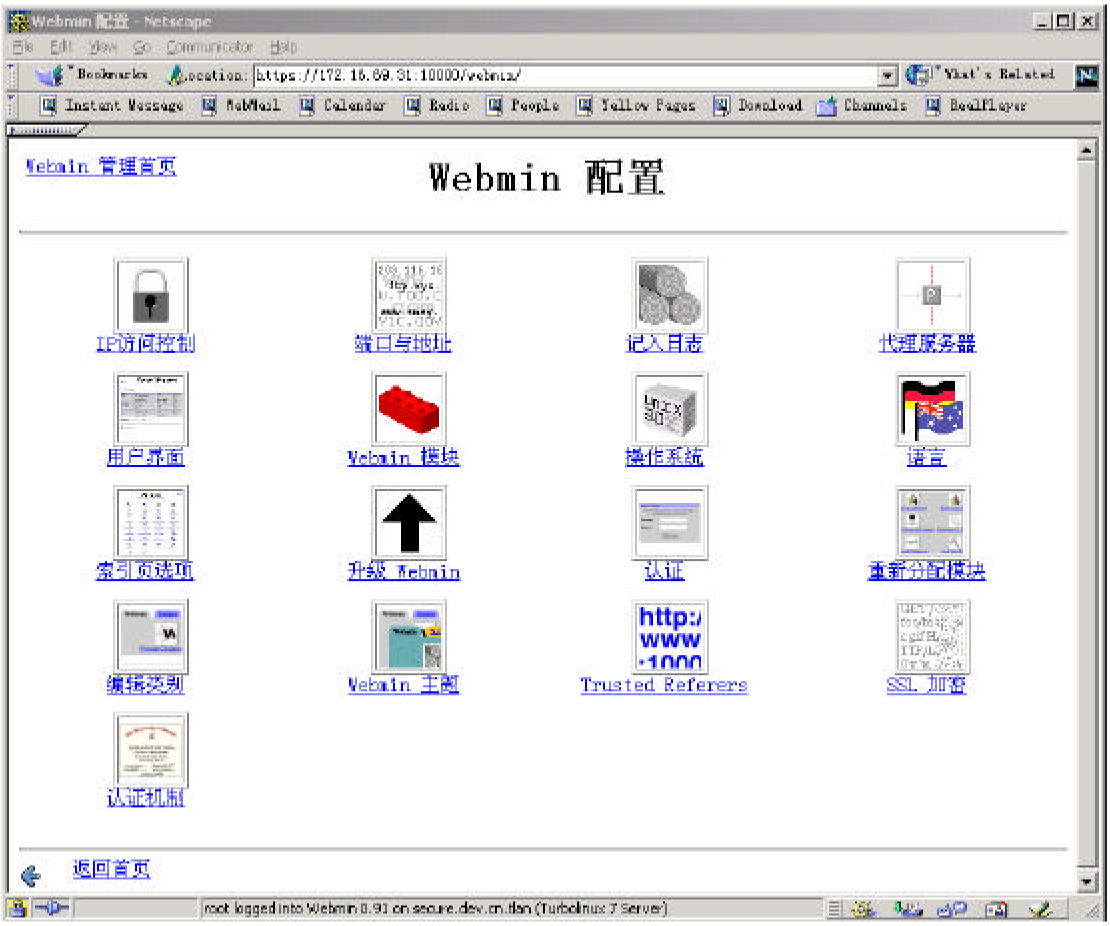
默认 webmin 的日志功能是关闭的，如果需要，请进入“webmin 活动日志”按照提示设置并开启 webmin 日志功能。

如果设置复选“每次日志的修改时所产生的文件”，那么，您在查询日志时就可以同时看到哪些文件被修改以及如何修改的。这也是学习 turbolinux 文件配置的一个技巧。

Turbolinux 安装的 webmin 默认使用简体中文，如果需要更改请选择“webmin 配置”的“语言”。

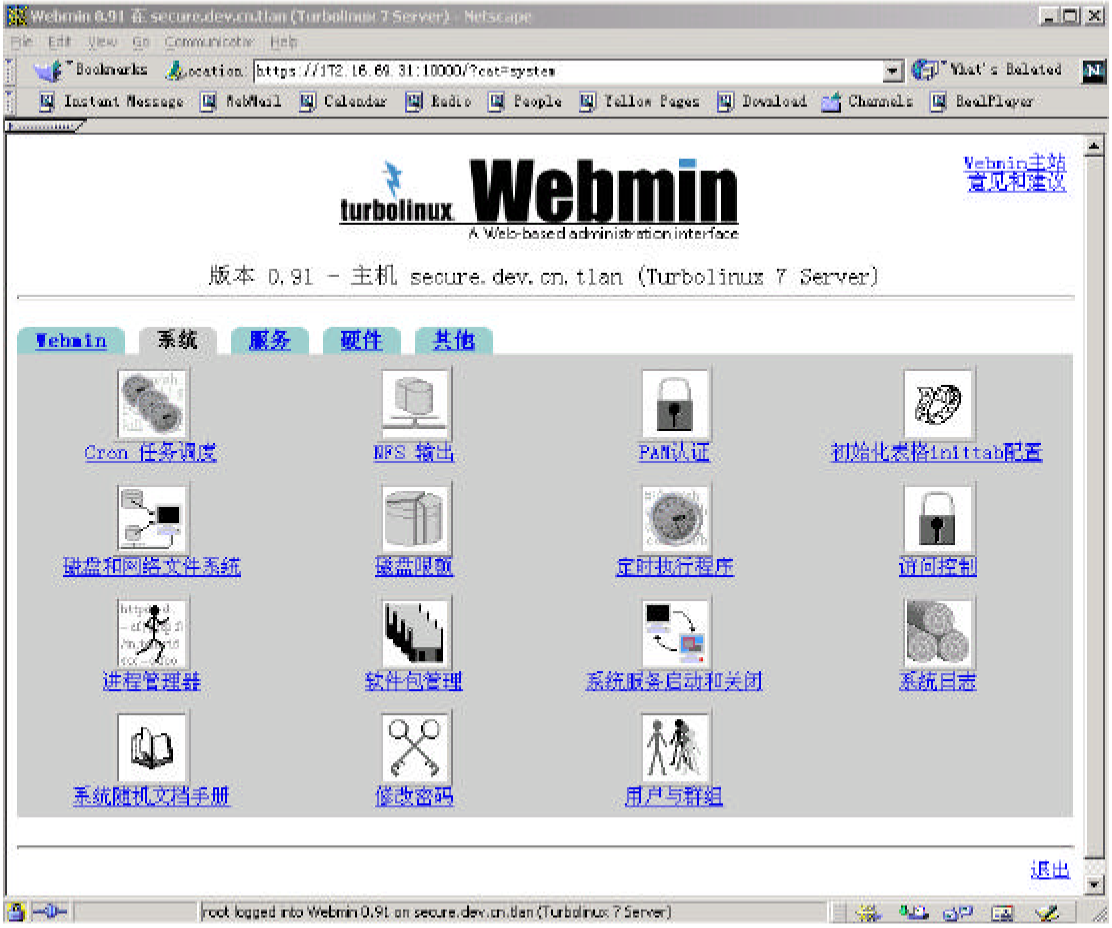
如果您使用有 java 功能的模块时，该模块中有可能不能显示中文内容，请选择语言为英文，然后再使用该功能模块。

所有 webmin 本身的管理和配置工作都可以在这里进行。



8.5 系统管理

这里完成的主要是系统本身的配置，具体功能见图片下面的表格。



模块	功能
Cron 任务调度	添加、创建、修改 Cron 任务
NFS 输出	添加、创建、修改 NFS 共享目录(依赖 portmap)
PAM Authentication	PAM 认证的配置，涉及网络安全。
初始化表格 inittab 配置	Turbolinux 系统初始化过程配置，也可以直接修改 /etc/inittab 文件达到相同目的。
磁盘和网络文件系统	用户本地或网络磁盘、共享文件系统的加载、卸载等操作。
磁盘限额	用于限制普通帐户对磁盘空间的使用，防止磁盘空间溢出。
定时执行程序	定时执行程序(at 命令)
访问控制	服务器主机访问控制,修改文件/etc/hosts.allow.
进程管理器	显示当前系统中进程的详细状态，并可以对这些进程发送 HUP 等信号或设置不同的优先级等操作。
软件包管理	软件包管理（rpm）
系统服务启动和关闭	系统服务启动,关闭及重启，关闭机器
系统日志	系统日志查看及日志第统配置
系统随机文档手册	可用关键词搜索 MAN 手册，HOWTO 文档等
更改密码	改变已有系统用户的密码
用户与群组	增加、修改、删除系统中的用户和用户组

8.6 服务

这里用于各种系统服务和守护进程的设置，具体功能见图片下面的表格。

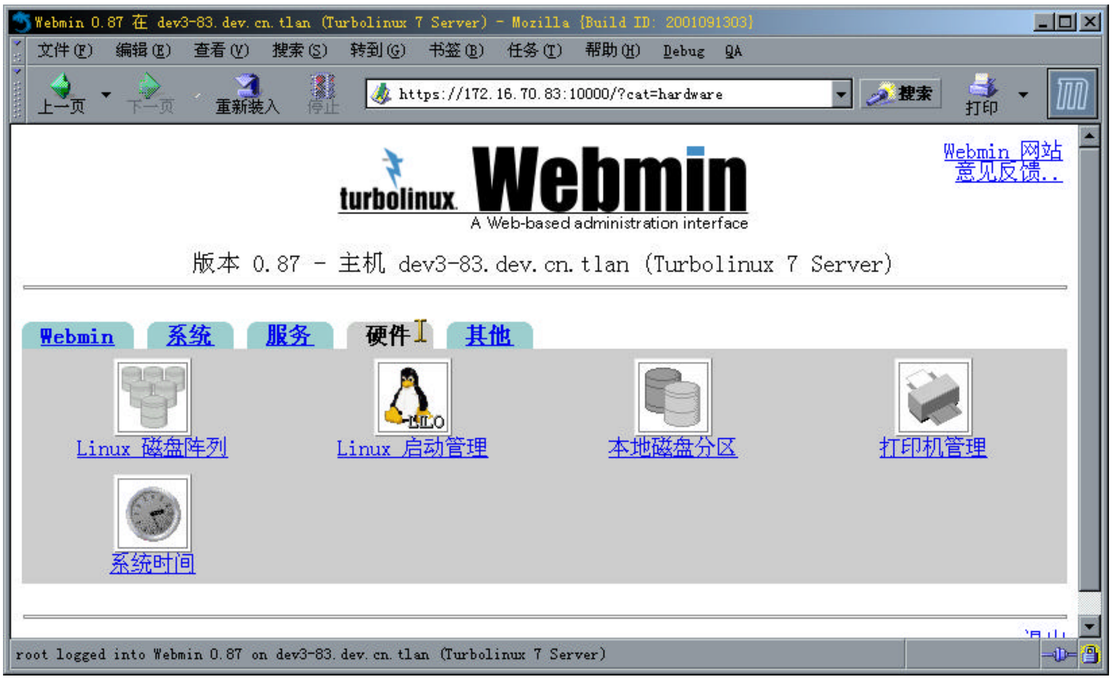


模块	功能
Apache 网页服务器	web 服务器 Apache 的设置
BIND DNS 服务器	bind 8，域名服务配置
DHCP 服务器	动态 IP 地址分配服务， DHCP 的配置，管理
Majordomo 列表管理	邮件列表管理，Turbolinux 没有安装该软件
MySQL 数据库服务器	MySQL 数据库的建立、修改、删除、权限管理及 MySQL 服务的启动和停止
PPP 帐户	调制解调器播入拔出帐号的增加、删除、修改
PostgreSQL 数据库服务器	PostgreSQL, Turbolinux 没安装
Proftpd FTP Server	Turbolinux 默认的 ftp 服务软件，等同于直接修改文件配置文件 proftpd.conf
SSH Server	配置，管理远程 SSH 终端
Samba Windows 文件共享	配置，管理和 win9x 兼容的文件夹共享机制
Sendmail 配置	配置，管理 Sendmail 邮件服务器
Squid 代理服务器	配置，管理 Squid 代理服务软件
Xinetd 服务配置	Turbolinux 使用的扩展的 internet 超级服务器软件
Fetchmail Mail Retrieval	邮件提取转发程序(需启动 sendmail)

inetd 服务配置	默认不再使用
Snort 网络入侵监测系统	配置，管理 Snort 网络入侵监测系统

8.7 硬件设置

这部分是和硬件、外设相关的设置。



模块	功能
Linux 磁盘阵列	建立、删除 linux soft raid
Linux 启动管理	创建、删除、修改系统启动时可使用的操作系统以及参数(lilo.conf)
本地磁盘分区	本地硬盘分区及参数优化设置，注意，错误操作将破坏硬盘上的数据！
打印机管理	配置本地或远程打印机
系统时间	读取、设置、同步本地系统或硬件时钟，例如可以使用 clock.sgi.com 的标准时间同步本地时钟

8.8 其他

这里是一些常用的工具模块，很多需要 java 的支持。



Perl 模块	从本地或网络增加新的 Perl 模块组
SSH/Telnet 登录	在你的浏览器中运行 SSH/Telnet 远程终端
文件管理器	在你的浏览器中打开一个图形界面的文件管理器
系统和服务器的状态	可以监视各种服务和系统的状态
用户自定义命令	增加，删除常用命令或文件编辑的快捷图标
执行命令	执行 linux 的 shell 命令并显示返回的结果

第九章　数据库

9.1 TDS 7 上安装 SYBASE 11.9.2

因为 SYBASE 11.9.2 的 RPM 包定义了倚赖关系 ld.so >= 1.9.5-8.so。 在 TDS 7 中 glibc 2.2.4 将 ld.so 重命名为 ld-linux.so，所以需在手工安装 SYBASE 11.9.2 的 RPM 包时加上 --nodeps 参数即可。

9.2 Turbolinux 7 DataServer 上安装 Oracle 8i Release 2 (8.1.7)的方法

Oracle 9i 能不加修改地顺利安在 Trubolinux 7 DataServer 上。但于，Oracle 8i for Linux 是在 glibc 2.1.3 上开发的, 直接在 Trubolinux 7 DataServer 下的 libc 2.2.4 上安装在链接阶段会失败。要正确安装 Oracle 8i 需作以下工作。

1) 升级 binutils
   在 Turbolinux Database Server 7 中的 binutils 版本为 2.11.90.0.23 需升级至 2.11.92.0.7 此 rpm 包在安装光盘的目录 addons/Ora8i 下。

2) 安装 compat-glibc
   此 rpm 包为 glibc 2.1.3-1 的兼容包,在安装光盘的 addons/Ora8i 下。

3) 按照安装光盘中的 addons/Ora8i/README 所述步骤继续安装。
   1. 以 oracle 用户身分执行安装至创建数据库阶段,然后放弃安装。
   2. 以 oracle 用户身分执行 resetup.sh 脚本,注意 unset LD_LIBRARY_PATH 环境变量。
   3. 用 dbassist 工具创建数据库(需设置环境变量 LC_ALL,LANG 为 C,否则在中文语言环境下,dbassist 将产生 segment fault)。
   4.

9.3 Oracle 工具包 TOra

TOra 是面向数据库开发人员和 DBA 的 Oracle 工具.它受到 Windows 下 TOra 的影响.它包涵模式浏览器,SQL 工作表格,PL/SQL 编辑器与调试器,存储管理器,回滚段监视器,实例管理器和 SQL 输出查看器.

模式浏览,模式浏览功能可以让我们快速访问数据字典，浏览数据库中的表、索引、存储过程。TOra 提供对数据库的快速访问，使用极为方便，用户界面简洁，结构安排合理。当我们点击一个单独的数据库对象，TOra 立即显示此对象的详细信息。例如，当我们点一个数据库的表，所有和此表相关的索引、约束、存储过程、SQL 语句以及和其他表的相互引

用关系都在同一界面显示出来。为了简化操作，用户可以在浏览窗口操作数据库对象。

SQL 编辑器包括一个编辑窗口和运行结果窗口，允许开发人员在编辑的过程中测试运行结果。SQL 编辑器中不仅包括标准的编辑命令，也包括一些增强的功能，如快速查询表中的字段、将 SQL 语句的内容格式化等等。这个窗口可以处理大到 4GB 的内容，对大的开发项目来说非常有用。便捷的书签可以让开发人员非常容易地找到相关位置。在运行结果窗口可提供用户定义的配置功能，支持 LONG 和 LONG RAW 列，可以将数据卸出到磁盘、打印数据、编辑数据等等。

存储过程编辑器,存储过程编辑器的主要功能是编辑、编译、测试、调试存储过程和触发器。TOra 提供语法标识、错误标识和其他很多易于使用的功能，如在弹出窗口显示表名、列名和 Oracle 函数。和其他的 PL/SQL 编辑工具不同，TOra 允许在一个文件中操作多个数据库对象，可以编译一个对象、编译多个对象、编译到当前光标、从光标开始编译。在运行出现错误时，存储过程停止到有问题的语句。用户可以使用快捷方式或模板来快速编写 PL/SQL,也可以根据需要生成自己的模板。使用 TOra 可以非常方便地进行编辑工作，可如设置书签、取消注释、格式化 SQL 语句等等。

PL/SQL Debugger 选项，TOra 提供简单易用的 PL/SQL 调试功能，可以节省开发人员在大型项目中用于开发和测试的宝贵时间，提高应用开发的质量。在存储过程开发的过程中，TOra 可以逐行编辑、调试和运行代码。运行时可以根据需要输入参数，观察相关参数的变化来检查存储过程的正确性。在调式过程中，TOra 可以通过窗口显示所有的断点、参数，调用堆栈和输出参数。使用 TOra，非常容易检测到存储过程的错误，开发人员可以一步一步运行 PL/SQL 语句来识别问题。调试会话可以和其他程序会话同时进行。

启动命令:

```
#>tora
```

注意：设置环境变量 ORACLE_HOME,ORACLE_SID

9.4 unixODBC

unixODBC 所有的程序基于 GPL,所有的开发库基于 LGPL (除 nn 外,它基于 GPL?)。unixODBC 被看作由许多组件组成的单一的软件。unixODBC 项目的目标为开发和完善 unixODBC 使之成为 Linux 平台上的 ODBC 的标准。unixODBC 为 Linux 平台提供完整的 ODBC 解决方案。unixODBC 包含 ODBC Driver 管理器和工具(如:dltest,isql 和 odbcinst)

9.4.1 odbcinst 用法:

odbcinst 安装程序和卸载程序。更新系统文件,增加减少使用计数但并不真的复制或删除任何文件。

odbcinst 用法

odbcinst 操作 目标 选项

操作: -i 安装 -u 卸载 -q 查询

目标:　-d 驱动　-s 数据源
选项:　-f 文件名(与-i 一起使用)
　　　　-n 驱动或数据源名称(与-u 一起使用)
　　　　-v 关闭冗余显示(没有信息,警告或错误信息)
返回值: 0　成功　!0　失败　*

更详细信息请访问: http://www.unixodbc.org

例如:

```
odbcinst -i -d -f templatefordriver.ini
odbcinst -i -s -f templatefordatasource.ini
odbcinst -q -d
odbcinit -q -s
```

templatefordriver.ini 文件内容:

```
[MySQL]
Description= ODBC for MysQL
Driver= /usr/lib/libmyodbc.so
Setup= /usr/lib/libodbcmyS.so
FileUsage= 1
```

templatefordatasource.ini 文件内容:

```
[testmysql]
Description= ODBC test DSN for MySQL
Driver= MySQL
Trace= Yes
TraceFile= /tmp/testmysql.log
Server= localhost
Port=
Sockets=
Database= testdb
```

9.4.2　isql 的用法:

语法: isql DSN [UID [PWD]] [选项]
选项:　-b　批处理,没有提示符
　　　　-dx　以字符 x 分隔列
　　　　-w　将结果存于 HTML 表中
　　　　-v　冗余显示(显示提示信息,警告和错误信息)

注意:在批处理模式下 isql 支持重定向和管道操作

例子: cat My.sql | isql WebDB MyID MyPWD -w*

在 My.sql 文件中每一行必需包含一个 SQL 语句,最后一行必需为空
更详细信息请访问: http://www.unixodbc.org
例如: isql testmysql

9.4.3 dltest 的用法

语法: dltest libName Symbol
libName 完整路径加共享库名
Symbol 共享库内的函数名

注意: 此程序可用于在 makefile 中,当遇到测试失败则抛出出错信息

例子: dltest /usr/lib/libMy.so MyFunc
更详细信息请访问: http://www.unixodbc.org
例子: dltest /usr/lib/libodbcpsql.so ODBCINSTConstructProperties

9.4.4 gODBCConfig

gODBCConfig 包含 gODBCConfig 图形工具,它是基于 GTK+的 ODBC 配置工具。
用法:gODBCConfig
要点:先配置 ODBC 驱动,然后配置相应的 DSN(Data Source Name)

配置驱动包含两步(除填写相应的 ODBC 驱动名称和描述外):

第一步是:配置相应的 ODBC 驱动
以 PostgreSQL 为例:在 Driver 栏填写:/usr/lib/libodbcpgsql.so
第二步是:配置相应的 ODBC 驱动设置
以 PostgreSQL 为例:在 Setup 栏填写:/usr/lib/libodbcpgsqlS.so
配置结束后,会在/etc/odbcinst.ini 文件中添加如下的记录:

```
[PostgreSQL]
Description  = ODBC for PostgreSQL
Driver       = /usr/lib/libodbcpsql.so
Setup        = /usr/lib/libodbcpsqlS.so
FileUsage    = 1
```

配置相应的 DSN(Data Source Name),分为两步:

第一步是:选择相应的 ODBC 驱动
例如:在此步选择前面设置的 PostgreSQL ODBC 驱动
第二步是:填写相应的 ODBC 驱动设置内容.
例如:填写 DSN 名称,DSN 描述,Trace 文件,数据库,服务器名,用户名,口令,等等
配置结束后,会在相应文件中添加如下记录:

```
[testpostgresql]
Description= PostgreSQL
Driver= PostgreSQL
Trace= Yes
TraceFile= /tmp/testpostgresql.log
Database= testdb
```

```
Servername= localhost
UserName= postgres
Password=
Port= 5432
Protocol= 6.4
ReadOnly= Yes
RowVersioning= Yes
ShowSystemTables= Yes
ShowOidColumn= Yes
FakeOidIndex= Yes
ConnSettings=
```

DSN 分为 User DSN 和 System DSN
User DSN 只有用户自己可用.默认为$HOME/.odbc.ini 文件
System DSN 所有用户都可使用.默认为/etc/odbc.ini

配置成功以后,可用 isql 命令进行检验。

9.4.5 unixODBC 驱动和驱动配置

unixODBC 安装了如下驱动和驱动配置:

```
unixODBC-filedsn       基于文件的数据源的 ODBC 驱动配置(基本)
        文件           /usr/lib/libodbcdrvcfg2S.so
unixODBC-generic       基于服务器的数据源的 ODBC 驱动配置(基本)
        文件           /usr/lib/libodbcdrvcfg1S.so
unixODBC-mysql         MySQL 数据库的 ODBC 驱动配置
        文件           /usr/lib/libodbcmyS.so
unixODBC-news          Internet News Server 的 ODBC 驱动和驱动设置
        文件           /usr/lib/libnn.so(驱动)
                       /usr/lib/libodbcnnS.so(驱动设置)
unixODBC-oracle8       Oracle 数据库 ODBC 驱动设置
        文件           /usr/lib/liboraodbcS.so
unixODBC-postgresql    PostgreSQL 数据库 ODBC 驱动和驱动设置
        文件           /usr/lib/libodbcpsql.so(驱动)
                /usr/lib/libodbcpsqlS.so(驱动设置)
unixODBC-sybase        Sybase 数据库 ODBC 驱动设置
        文件           /usr/lib/libtdsS.so
unixODBC-template      ODBC 驱动模板
        文件           /usr/lib/libtemplate.so
unixODBC-text          文本文件 ODBC 驱动
        文件           /usr/lib/libodbctxt.so
```

9.4.6 unixODBC 驱动配置实例

以 MySQL 为例:
在 unixODBC 中只包含 MySQL 数据库 ODBC 驱动配置,不包含 MySQL 数据库驱动,因此需到 http://www.mysql.com 下载 MyODBC 驱动.

下载了 MyODBC-2.50.37.tar.gz
执行以下配置命令:

```
#cd /tmp
#tar zxvf MyODBC-2.50.37.tar.gz
#cd MyODBC-2.50.37
#./configure --prefix=/usr --with-unixODBC=/usr
--with-mysql-dirs=/usr/lib/mysql --with-mysql-includes=/usr/include/mysql
--with-odbc-ini=/etc
#make
#make install
```

安装之后执行 gODBCConfig 配置 MySQL 驱动和 DSN,用 isql 检验.